VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH DOPORUČENÝCH POSTUPŮ PRO ZAJIŠTĚNÍ INFORMAČNÍ BEZPEČNOSTI V MALÝCH ZDRAVOTNICKÝCH ZAŘÍZENÍCH

BEST PRACTICES OF INFORMATION SECURITY FOR SMALL HEALTH FACILITIES

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Bianka Fábryová

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Viktor Ondrák, Ph.D.

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Bianka Fábryová**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2019/20

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Návrh doporučených postupů pro zajištění informační bezpečnosti v malých zdravotnických zařízeních

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout management bezpečnosti.

Základní literární prameny:

CALDER, A. a S. WATKINS. Information Security Risk Management for ISO 27001/ISO 27002. 3. ed. Cambridgeshire: It Governance Publishing, 2019. ISBN 978-1-78778-137-5.

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.

ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.

HERZIG, W. T., T. WALSH and L. A. GALLAGHER. Implementing Information Security in Healthcare: Building a Security Program. Chicago: HIMSS, 2013. ISBN 978-1-938904-35-6.

HERZIG, W. T. Information Security in Healthcare: Managing Risk. Chicago: HIMSS, 2010. ISBN 978-1-938904-01-1.

POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-8--7251-250-8.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Cieľom tejto práce je návrh odporúčaných postupov informačnej bezpečnosti so zameraním na malé zdravotnícke zariadenia a ochranu dát pacientov. Úvodná časť práce sa sústredí na zhrnutie teoretických východísk z oblasti informačnej bezpečnosti, ktorých ťažiskom je séria noriem ČSN ISO/IEC 27000. V praktickej časti je na základe aplikácie teoretických poznatkov formulovaný návrh odporúčaných postupov a konkrétne kroky, ktoré by mali zdravotnícke zariadenia učiniť pre dodržanie zásad informačnej bezpečnosti.

Kľúčové slová

ISMS, informačná bezpečnosť, ISO/IEC 27000, bezpečnostné normy, ochrana dát, zdravotnícke zariadenia, bezpečnostná politika, bezpečnosť ICT

Abstract

This thesis deals with proposal of best practices of Information Security focusing on small medical facilities and data protection of the pacients. The introductory part of this thesis focuses on the theoretical background of information security, based on the series of standards ISO/IEC 27000. In the practical part, based on the application of theoretical knowledge, there is formulated a proposal of recommended steps health care facilities should take to compliance with the principles of information security.

Keywords

ISMS, information security, ISO/IEC 27000, security standards, data protection, medical facilities, security policy, ICT security

Bibliografické citácia

FÁBRYOVÁ, Bianka. *Návrh doporučených postupů pro zajištění informační bezpečnosti v malých zdravotnických zařízeních* [online]. Brno, 2020 [cit. 2020-05-07]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/125739. Bakalárska práca. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedúci práce Ing. Viktor Ondrák, Ph.D.

Čestné prehlásenie

Prehlasujem, že predložená bakalárska práca je pôvodná a spracovala som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušila autorské práva (v zmysle Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brne dňa 7. mája 2020 .....

podpis autora

Poďakovanie

Ďakujem vedúcemu bakalárskej práce, Ing. Viktorovi Ondrákovi, Ph.D., za odborné vedenie, cenné rady a ústretový prístup pri písaní tejto práce. Rovnako sa chcem poďakovať svojim rodičom za ich podporu pri štúdiu a Ing. Zoňovi za konzultácie, ktoré mi pomohli pri tvorbe tejto práce.

Obsah

ÚVOD

S rozmachom informačných technológií sa čoraz viac údajov sústredilo v informačných systémoch a s príchodom informatizácie sa množstvo činností a informácií presúva do virtuálneho priestoru. Z tohto faktu však vyplýva, že takéto dáta podliehajú vysokej miere ochrany, nakoľko ich zneužitie môže mať neraz až fatálne dôsledky. Z médií dnes častokrát počúvame správy o únikoch dát, ktorým sa nevyhli ani organizácie, ktoré považujeme za bezpečné, ako napríklad banky, vládne inštitúcie a úrady, či mobilní operátori. Riziku takéhoto napadnutia však čelia inštitúcie a organizácie naprieč celým spektrom. Útočníci sa zaujímajú predovšetkým o osobné údaje, bankové a obchodné dáta, či iné, často kľúčové informácie spoločností. Hrozieb, ktorým v tejto oblasti čelíme, však existuje viacero a častokrát ich pôvodcami nie sú útočníci, ale práve ľudia, ktorým sú údaje priamo dostupné, a ktorí svojou nedbanlivosťou a neznalosťou napomáhajú k ich vzniku. Predmetom informačnej bezpečnosti je týmto incidentom predchádzať, znižovať riziko ich vzniku, znižovať ich dopady a neustále celý systém monitorovať, k čomu nám slúžia overené postupy a normy.

S citlivými dátami, osobnými údajmi, sa stretávame v každodennom živote a zdravotná starostlivosť tvorí nepochybne ich majoritnú časť. Zdravotnícke zariadenia počas svojej činnosti vo veľkej miere prichádzajú do styku s citlivými údajmi pacientov, vytvárajú ich a ukladajú vo svojich informačných systémoch. Elektronická dokumentácia prináša na jednej strane efektivitu, nakoľko vedie k oveľa rýchlejšej a bezpečnejšej ceste k liečbe pacientov, na druhej strane však stojí riziko vystavenia ich súkromia. Informácie zdravotnej dokumentácie sú považované za jedny z najcitlivejších vôbec, a aj z tohto dôvodu podliehajú takéto zariadenia množstvu legislatívnych a normatívnych predpisov. Vychádzajúc z osobných skúseností viem, že zdravotnícke zariadenia vo veľkej miere túto problematiku ignorujú, i keď to nie je cielené, zatiaľ si neprivykli na možnosť narušenia bezpečnosti informačného systému, a preto ju mnohokrát nepovažujú za podstatnú a potrebnú. Ich názor sa mení zvyčajne až v bode, keď im niekto z auta ukradne notebook, keď im zlyhá pevný disk na počítači bez možnosti záchrany dát, alebo keď stratia dáta za niekoľko mesiacov práce, zatiaľ čo po zálohách niet ani stopy, pričom dopad nemusí byť len finančný, ale aj morálny, či klinický. Aj keď je táto problematika

pomerne dobre legislatívne a normatívne podchytená a venuje sa jej čoraz viac ľudí, pravdou zostáva, že je to stále nedostatočné.

Táto bakalárska práca sa bude zaoberať informačnou bezpečnosťou pri narábaní a uchovávaní dát v súvislosti so zameraním na zdravotnícke zariadenia a ochranu dát pacientov. Prvá časť práce popisuje teoretické východiská, ako pojmy z oblasti informačnej bezpečnosti, normy a právne požiadavky, riziká a bezpečnostnú politiku a systém zavádzania informačnej bezpečnosti. Praktická časť práce obsahuje analýzu skutočného stavu bezpečnosti vo vybraných medicínskych zariadeniach a analýzu rizík. Na základe týchto analýz budú následne v praktickej časti tieto východiská aplikované na konkrétne kroky a bude vytvorený návrh doporučených postupov pre zaistenie informačnej bezpečnosti v malých zdravotníckych zariadeniach.

1. VYMEDZENIE PROBLÉMU A CIEĽ PRÁCE

Práca sa zameriava na problematiku managementu informačnej bezpečnosti v zdravotníctve. Cieľom tejto práce je vytvorenie návrhu doporučených postupov pre zaistenie informačnej bezpečnosti v malých zdravotníckych zariadeniach s využitím noriem ISO 27000. Na základe analýz prístupu k informačnej bezpečnosti niekoľkých vybraných zariadení bude skompletizovaný pohľad na súčasný stav, čo bude spolu a analýzou rizík a s teoretickou a legislatívnou bázou slúžiť ako podklad k tvorbe návrhu postupov.

Môj návrh nie je komplexným riešením zahŕňajúcim všetky prvky, o ktorých pojednávajú normy ISO o informačnej bezpečnosti. Zameriava sa na body a aspekty, ktoré sú dôležité práve pre dodržanie informačnej bezpečnosti v malých zdravotníckych zariadeniach, s ohľadom na primerané technické, finančné a personálne náklady. Medzi zdroje, z ktorých pri tvorbe tejto práce čerpám, patria normy ISO, zákonné požiadavky a odborná literatúra zaoberajúca sa touto problematikou.

2. TEORETICKÉ VÝCHODISKÁ PRÁCE

Táto práca pojednáva o informačnej bezpečnosti v kontexte malých medicínskych ambulantných zariadení. Na úvod je preto potrebné vymedziť pojem informačná bezpečnosť a k nej priľahlé zložky. V nasledujúcich podkapitolách sa budem venovať popisu pojmov z oblasti informačnej bezpečnosti, ich fyzickým aj logickým aspektom, legislatívnym a normatívnym požiadavkám, ako aj managementu bezpečnosti informačných systémov.

2.1. Pojmy informačnej bezpečnosti

2.1.1. Dôležitosť informačnej bezpečnosti v zdravotníctve

S príchodom informačných technológií a elektronizácie do zdravotníckej sféry sa problematika bezpečnosti citlivých dát ešte viac prehlbuje. Zdravotnícke zariadenia, ktoré doteraz bezpečnosť dát neriešili vôbec, sú postupne nútené, aby sa o túto oblasť začali aktívne zaujímať, aj keď je ich záujem skôr spôsobený rešpektom pred finančnou ujmou, než samotným záujmom o bezpečnosť informácií. Je nutné podotknúť, ako veľmi špecifická je práve situácia v zdravotníctve. Pred dvadsiatimi rokmi bola k internetu pripojená len hŕstka ľudí, takmer vôbec neexistovala potreba zápisu citlivých údajov v elektronickej forme, lekári štandardne zapisovali záznamy do kariet pacientov na písacích strojoch a výkazníctvo bolo taktiež vo svojich začiatkoch. Len málo lekárov sa naozaj naučilo pracovať so zdravotníckym softvérom, väčšinou túto prácu vykonávala iná osoba. Samotné databázy, ktoré vtedy vznikali, boli častokrát nezabezpečené, dáta nezašifrované, no rovnako aj možnosť odcudzenia a zneužitia databázy bola menšia ako v súčasnosti. Problematiku bezpečnosti nikto v tej dobe neriešil. Dnes je však väčšina spracovávaných dát elektronizovaná a posielajú sa ako medzi jednotlivými pracoviskami lekárov a nemocničnými zariadeniami, tak medzi poisťovňami, laboratóriami, do NCZI (Národné centrum zdravotníckych informácií), pacientom samotným a rôznym iným zariadeniam. Tieto špecifické údaje zahŕňajú prakticky kompletný popis pacienta, vrátane jeho zdravotného, geografického, sociálneho určenia, kontaktov a mnohého iného. Dáta sú zdrojom najcennejšieho aktíva medicínskych zariadení. A preto je nevyhnutné, aby lekári venovali patričnú pozornosť ich zabezpečeniu, čo aj im samým prinesie nemalé

zlepšenie efektivity práce. Samotné dáta musia byť síce chránené s vysokým stupňom vážnosti, no zároveň musí byť splnená aj podmienka ich dostupnosti, predovšetkým ak sa jedná o sektor zdravotníctva. Je preto potrebné nájsť rovnováhu medzi bezpečnosťou, cenou a použiteľnosťou celého systému. Musíme zhodnotiť nehmotnú cenu a dôležitosť aktív, zhodnotiť cenu náhrady či straty aktíva a ustanoviť vhodné spôsoby a metódy ich zabezpečenia. Každá organizácia, aj tá medicínska, musí mať nastavené pravidlá bezpečnosti aj pre najbežnejšie činnosti, nakoľko je potrebné uvedomiť si, že bezpečnosť nezávisí len na zabezpečení technológií, ale dotýka sa aj fyzického zabezpečenia budovy, priestorov, právomocí, prístupov, činností a mnohých ďalších aspektov.

V skutočnosti neexistuje nič také ako úplne zabezpečený systém. To však neznamená, že by sme nemali podniknúť kroky k jeho zabezpečeniu. Odvďačí sa nám to prostredníctvom mnohých benefitov, ktorými sú kvalitnejšia a dôveryhodnejšia organizácia, minimalizácia rizika úniku či straty dát, ochrana samých seba, dobrého mena, zamestnancov a pacientov, ktorí budú mať záruku, že nedôjde k narušeniu bezpečnosti ich údajov. Investícia do informačnej bezpečnosti napomáha k predchádzaniu neočakávaných udalostí, znižuje mieru dopadu incidentov a z nich plynúce finančné náklady.

2.1.2. Všeobecné pojmy bezpečnosti ICT

Aby sme mohli situáciu v medicínskych zariadeniach zasadiť do problematiky informačnej bezpečnosti, je potrebné priblížiť niektoré pojmy z tejto oblasti.

- **Dostupnosť** (*availability*) – zabezpečenie, že informácie sú dostupné pre používateľov informačného systému v momente, kedy to potrebujú,
- **Dôvernosť** (*confidentiality*) – zabezpečenie, že k informáciám majú prístup len oprávnení používatelia informačného systému,
- **Integrita** (*integrity*) – zabezpečenie presnosti a celistvosti informácií,
- **Informačná bezpečnosť** (*information security*) – je to systém ochrany informácií, dosahovaný prostredníctvom zachovania jej základných atribútov, teda dostupnosti, dôvernosti a integrity informácií,

- **Informačné aktívum** (*information asset*) – všetko, čo má pre organizáciu hodnotu a význam. Aktíva môžu byť hmotné (počítačové vybavenie) alebo nehmotné (povesť),
- **Bezpečnostná hrozba** (*security threat*) - je stav, ktorý má nepriaznivý vplyv na informačné aktívum. Ak hrozba pôsobí na zraniteľné miesto aktíva, môže byť príčinou vzniku bezpečnostnej udalosti alebo incidentu,
- **Bezpečnostná udalosť** (*security event*) - je stav, kedy mohlo dôjsť k situácii, ktorá môže znamenať narušenie bezpečnosti informácií,
- **Bezpečnostný incident** (*security incident*) - bezpečnostný incident je nežiaduca bezpečnostná udalosť, ktorá môže spôsobiť významné narušenie činností organizácie a narušenie dostupnosti, dôvernosti alebo integrity,
- **Riziko** (*risk*) – riziko je pravdepodobnosť, s akou môže konkrétna hrozba pôsobiť na zraniteľnosť aktíva a potencionálne spôsobiť škody,
- **Bezpečnostné opatrenie** (*security safeguard*) – prijatie prostriedkov alebo činností, ktoré modifikujú riziko,
- **Autorizácia** (*authorization*) – jedná sa o proces, pri ktorom sú osobe alebo systému poskytnuté práve tie služby, pre ktoré je oprávnený,
- **Autentizácia** (*authentication*) – jedná sa o záruku, že stanovená charakteristika entity je korektná,
- **Autenticita** (*authenticity*) – vlastnosť, ktorá zaručuje prehlasované charakteristiky entity za autentické (1).

2.1.3. Informačný systém

Informačný systém nemá danú jednoznačnú definíciu. Všeobecne ho ľudia chápu ako miesto v organizácii, kde sa zhromažďujú, uchovávajú, spracovávajú a poskytujú dáta a informácie. Informačný systém je však lepšie definovať ako súbor prvkov s určitými vzájomnými väzbami a so špecifickým správaním (2). Prvky, ktoré systém zahŕňa, sú technické, personálne a organizačné. Úlohou informačného systému je efektívne

poskytovať jeho oprávneným užívateľom služby, akými sú napríklad zber, spracovanie, prenos, či uchovávanie dát (3).

2.1.3.1. Prvky informačného systému

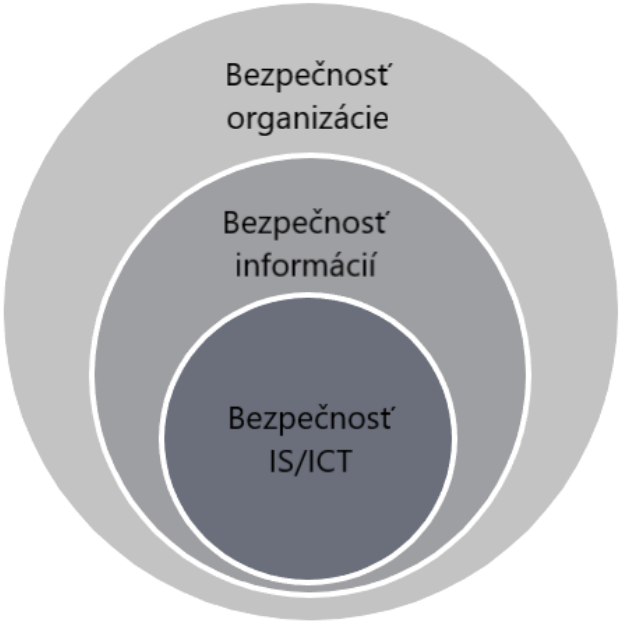
Hlavnou časťou informačného systému je po technickej stránke predovšetkým hardvér a softvér, ale okrem týchto sa skladá aj z ďalších prvkov, ktorými sú údaje, ľudia a organizačné súčasti, ktoré sú nemenej dôležité. Týmito zložkami sú:

- **Hardvér** (*hardware*) – všetky hmotné technické prostriedky, ktoré tvoria informačný systém, alebo sú jeho súčasťou. Musia byť kvalitné a pravidelne kontrolované, nakoľko práve od nich závisí kvalita poskytovaných služieb,
- **Softvér** (*software*) – všetky nehmotné technické prostriedky, ktoré tvoria informačný systém, alebo sú jeho súčasťou. Sú to programy, ktoré zaisťujú činnosti a poskytujú užívateľom služby,
- **Údaje** (*data*) – údaje, ktoré obsahuje informačný systém. Sú to dáta a informácie, ale aj znalosti ľudí,
- **Ľudia** (*peopleware*) – súbor ľudských vlastností, ktorý zabezpečuje chod informačného systému, udržiava ho a používa,
- **Organizačné súčasti** (*orgware*) – súbor pravidiel, ktoré upravujú zodpovednosti v spoločnosti (2).

2.1.4. Informačná bezpečnosť

Pojem bezpečnosť si všeobecne spájame s ochranou pred zničením, stratením, odcudzením či zneužitím. V informačnej bezpečnosti sa tieto pojmy priamo viažu s dátami. Jedná sa teda o ochranu dát pred zničením, stratou, krádežou, či ich zneužitím. V informačnej bezpečnosti však môžeme rozlišovať ochranu na niekoľkých úrovniach. Tou prvou je bezpečnosť organizácie ako takej, ktorá úzko súvisí s ochranou informácií. Je potrebné, aby boli chránené budovy a priestory organizácie, ako aj jej hmotný majetok. Takáto ochrana je zabezpečovaná predovšetkým fyzickými prostriedkami, ale dnes už aj rôznymi bezpečnostnými systémami, kamerami, či autentizačnými a snímacími zariadeniami. Druhou, užšou úrovňou v informačnej bezpečnosti je ochrana

informačných systémov a informačno-komunikačných technológií, ktorá sa sústredí priamo na vymedzenie a ochranu aktív organizácie (4).



Obrázok č. 1: Bezpečnosť organizácie, informácií a IS/ICT

(Zdroj: Vlastné spracovanie podľa: 4)

Jednoznačne môžeme tvrdiť, že na to, aby sme mohli dodržiavať zásady informačnej bezpečnosti, musia zásady bezpečnosti existovať naprieč celou organizáciou. Spadajú sem teda oblasti, akými sú už spomínaná ochrana a zabezpečenie fyzických priestorov, ochrana fyzického majetku, technických prostriedkov a dokumentácie, patrí sem však aj bezpečnosť ľudských zdrojov, zaškolenie personálu, vnútorné bezpečnostné smernice, systém zálohovania a mnohé ďalšie. Pri procese tvorby bezpečnosti v organizácii je však potrebné zvážiť, akú mieru dopadu môžu mať jednotlivé narušenia bezpečnosti a adekvátne k tomu, s primeranými finančnými prostriedkami, zabezpečiť ochranu jednotlivých prvkov systému.

Riešenie informačnej bezpečnosti je náročným a nikdy nekončiacim procesom, ktorý nemôže byť tvorený všeobecne, a ktorý musí zodpovedať aktuálnemu stavu danej organizácie. Preto je potrebné, aby ako vedenie, tak aj všetok personál podporovali a dodržiavali zásady bezpečnosti, a aby sa vytvorený systém bezpečnosti neustále kontroloval, aktualizoval a zlepšoval.

2.1.4.1. Fyzická bezpečnosť

Koncept fyzickej bezpečnosti predkladá v širšom zmysle ochranu pred prírodnými a personálnymi hrozbami ešte pred tým, než nastanú. Jedná sa teda o ochranu pred hrozbami, akými sú prírodné živly a katastrofy a pred personálnymi hrozbami, medzi ktoré patrí neoprávnený fyzický prístup a s ním spôsobené poškodenie a narušenie informácií. Z tohto hľadiska je potrebné zabezpečiť budovy, kde je umiestnený informačný systém. Fyzickú ochranu dosahujeme vytvorením viacerých fyzických bariér, ako uzamykaná budova, či obklopenie miestnosti ďalšími miestnosťami. Zabezpečenie oblasti je taktiež podporené opatreniami, ktoré určujú a regulujú prístup oprávnených osôb. Sú nimi napríklad udelenie prístupu pre konkrétne osoby, obmedzenie prístupu do miestností, kde sa uchovávajú dôverné informácie, zavedenie mechanizmu autentizácie, akými sú napríklad prístupové karty, vytvorenie záznamu o prístupoch a ďalšie. K fyzickej bezpečnosti patrí aj zabezpečenie techniky. Tá by mala byť umiestnená tak, aby sa zabránilo k jej prístupu neoprávneným osobám a zároveň, aby sa znížili riziká hrozieb z prostredia. Medzi opatrenia patrí napríklad zabezpečenie, aby pri práci so zariadením nebolo možné sledovať informácie neoprávnenou osobou, zabezpečenie vybavenia pre ukladanie dát pred vonkajšími vplyvmi, ako je voda, oheň, prach, výpadok elektrického napájania, výpadok komunikácie prepätí v elektrickej sieti a voči ďalším fyzikálnym hrozbám a rovnako aj bezpečná likvidácia zariadenia. Ochrana pred prírodnými vplyvmi by mala byť navrhnutá špecialistom (5).

2.1.4.2. Bezpečnosť IS

Bezpečnosť informácií v informačných systémoch si vyžaduje vysoké nároky a požiadavky na tieto systémy. Mali by odrážať hodnotu informácií, ktoré nesú, a zároveň odrážať dopady rizík z nich plynúcich na činnosť organizácie. V prípade informačných systémov a komponentov, ktoré organizácii poskytuje dodávateľ, je potrebné špecifikovať a zdokumentovať požiadavky na bezpečnosť týchto systémov a informácií, predovšetkým ak k nim môže pristupovať, spracovávať, ukladať a prenášať ich aj poskytovateľ (5).

2.1.4.3. Komunikačná bezpečnosť

Komunikačná bezpečnosť je oblasť zaoberajúca sa ochranou informácií v sieťach a v sieťovom vybavení. Pod opatreniami v tejto oblasti rozumieme predovšetkým riadenie a kontrolu sietí a pripojených sieťových služieb. Medzi takéto opatrenia patrí ustanovenie postupov pre správu a riadenie sieťových zariadení, vytvorenie opatrení na zabezpečenie dôvernosti a integrity dát, ktoré sú prenášané sieťami, ochrana systémov a aplikácií a zaistenie dostupnosti sieťových služieb a pripojených počítačov. Systémy v sieti by mali byť autentizované a mali by byť zaistené postupy monitorovania činnosti. Rovnako by organizácia mala ustanoviť konkrétne postupy a opatrenia k ochrane prenášaných dát prostredníctvom komunikačných technológií (5).

2.1.4.4. Bezpečnosť ľudských zdrojov

V problematike informačnej bezpečnosti v zdravotníckych zariadeniach, ktorou sa zaoberá táto práca, je kľúčová predovšetkým bezpečnosť ľudských zdrojov, nakoľko aj personálna zložka môže byť potencionálnou bezpečnostnou hrozbou. Jedná sa predovšetkým o prípady pasívneho konania a chýb, ktorých sa dopúšťa personál, no je tiež jedným z najčastejšie sa vyskytujúcich hrozieb pre informačnú bezpečnosť. Táto hrozba sa zvyčajne ťažko rozpoznáva a rovnako ťažko sa aj zamedzuje jej pôsobeniu. Je preto potrebné prijať opatrenia, ktoré spočívajú predovšetkým v preverovaní totožnosti a schopností zamestnancov (do miery, v akej to umožňuje legislatíva), v určení jednoznačných zodpovedností personálu a v zaškolení personálu v oblasti pravidiel bezpečnostnej politiky (5).

2.2. Analýza rizík a bezpečnostná politika

2.2.1. Analýza rizík

Prvým nevyhnutným krokom k tvorbe informačnej bezpečnosti v organizácii je nepochybne analýza rizík. V procese analýzy rizík sa nejedná o ich elimináciu, nakoľko je to nemožné, ale o vymedzenie, aké riziká v organizácii existujú, čo nám umožňuje definovať, čo je prioritne potrebné chrániť. Výzvou v tejto oblasti je nájsť vhodnú mieru medzi finančnými a organizačnými potrebami a možnosťami organizácie a medzi jej bezpečnosťou.

V analýze rizík identifikujeme niekoľko krokov:

- **Vymedzenie účelu a hraníc –** prvým krokom pri tvorbe analýzy rizík je vymedzenie hraníc, teda zadokumentovanie všetkých aktív, ktoré budú súčasťou analýzy rizík. Zostavenie hraníc podlieha rozhodnutiu vedenia organizácie o tom, ktoré aktíva považujú za dôležité z hľadiska podnikateľskej a profesijnej činnosti, bezpečnosti informácií, z hľadiska vynaložených finančných zdrojov, alebo z hľadiska legislatívnych nariadení. Organizácia sa rozhoduje o účele, ktorý bude záväzným pre posudzovanie aktív,
- **Identifikácia informačných aktív –** analýza rizík musí obsahovať dokumentované ohodnotenie informačných aktív. V tomto bode je potrebné spísať všetky aktíva, ktoré majú hodnotu pre organizáciu z hľadiska stanoveného účelu. V prípade, že je to potrebné, môžeme v tomto kroku zoskupiť aktíva do logických celkov na základe spoločných atribútov a prijímať bezpečnostné opatrenia pre skupiny aktív,
- **Identifikácia hrozieb –** v tomto kroku pristúpime k identifikácii hrozieb. Hrozby určujeme predovšetkým zo zdrojov, ktoré s daným aktívom pracujú, vyznajú sa v ňom a vedia odborne a objektívne zhodnotiť potenciál hrozby. Ako základné druhy hrozieb môžeme vymedziť zavinenie človeka, zavinenie prostredia a prírodné zavinenie,
- **Identifikácia zraniteľných miest aktív –** identifikujeme slabiny, zraniteľné miesta ku všetkým zdokumentovaným informačným aktívam. Zvyčajne sa jedná o miesta, ktoré sú nedostatočne chránené nastavenými technickými či organizačnými opatreniami, prípadne nemajú žiadne,
- **Stanovenie pravdepodobnosti javu –** analyzujeme vzťah hrozby k zraniteľnosti aktíva a určíme pravdepodobnosť výskytu daného javu, teda pravdepodobnosť, že bude hrozba pôsobiť na zraniteľnosť aktíva. Pri určovaní pravdepodobnosti výskytu daného javu je tiež potrebné posúdiť, či je výskyt danej hrozby neúmyselný, náhodný alebo úmyselný a adekvátne k tomu prijať potrebné bezpečnostné opatrenia,
- **Analýza dopadu –** v tejto časti posudzujeme potencionálnu mieru dopadu, aká by vznikla narušením bezpečnosti aktíva. Miera dopadu je odhadovaná pomocou

vstupov, ktorými sú hodnota aktíva a výstupy analýzy hrozieb. Pri určovaní hodnoty dopadu je potrebné zohľadniť mnoho faktorov, predovšetkým dopad na integritu, dostupnosť a dôvernosť, dôležitosť aktíva pre organizáciu z hľadiska profesijnej činnosti, finančnej hodnoty, ziskov z aktíva, z hľadiska reputácie, či doby nápravy a iných,

- **Určenie rizika –** pri určovaní rizika vychádzame zo stanovenej hodnoty pravdepodobnosti a hodnoty dopadu. Zistené údaje o rizikách nám slúžia ako podklad prioritizácie pri alokovaní zdrojov do bezpečnostných opatrení,
- **Stanovenie opatrení –** na základe zistených faktov stanovíme adekvátne bezpečnostné opatrenia za akceptovateľné náklady (6).

2.2.2. Bezpečnostná politika a jej význam pre organizáciu

Bezpečnostná politika organizácie je súbor dokumentov definujúci sadu opatrení informačnej bezpečnosti schválenú vedením spoločnosti, teda stanovuje prístup organizácie k naplneniu cieľov bezpečnosti informácií. Opatrenia z nej vyplývajúce sú záväzné pre celú organizáciu, vedenie i zamestnancov.

Bezpečnostná politika by mala obsahovať:

1. definíciu, význam, rozsah a ciele informačnej bezpečnosti organizácie,
2. deklaráciu zámeru vedenia organizácie podporovať naplnenie stanovených cieľov informačnej bezpečnosti,
3. bezpečnostné zásady, princípy, postupy a prípadné špeciálne požiadavky,
4. definíciu všeobecných a špecifických zodpovedností v oblasti informačnej bezpečnosti v organizácii, vrátane postupov a povinností pri bezpečnostných incidentoch,
5. zoznam dokumentov, ktoré bližšie špecifikujú politiku informačnej bezpečnosti (7).

Politika informačnej bezpečnosti musí mať stanovené pravidlá preskúmavania a správy, a to v pravidelných intervaloch, predovšetkým vo vzťahu k zmenám v organizácii. Cieľom revízie je zabezpečiť vecnú aktuálnosť bezpečnostnej politiky a rovnako

zabezpečiť aj efektívnosť prijatých a používaných zásad a opatrení k aktuálnemu stavu spoločnosti (5).

2.3. Legislatíva a normy v oblasti informačnej bezpečnosti

Normy predstavujú súbor pravidiel a požiadaviek o vlastnostiach produktov, činností a o priebehu procesov s cieľom zaručenia požadovaných vlastností, ktorých výsledkom je štandardizácia. V oblasti informačnej bezpečnosti vzniklo mnoho medzinárodne uznávaných štandardov, ktoré jasne definujú postupy v riešenej problematike, čím veľmi uľahčujú implementáciu týchto štandardov v praxi. Slovenská republika prijíma tieto normy len ako odporúčania pre riešenie problematiky. Nemajú teda záväzný charakter, no je vhodné riadiť sa nimi, ak by sa organizácia chcela certifikovať v oblasti bezpečnosti informačných systémov. Na systém riadenia bezpečnosti informácií na Slovensku má však vplyv aj mnoho legislatívnych požiadaviek, obzvlášť v prípade zdravotníckych organizácií, kde sa tieto zákony špecializujú predovšetkým na ochranu osobných údajov pacientov.

2.3.1. Vybrané normy upravujúce bezpečnosť informácií

Normatívny základ v oblasti riadenia bezpečnosti informácií tvorí rad noriem ISO/IEC 27000, ktorý vychádza od roku 2005, a ktorého tvorcom je Medzinárodná organizácia pre normalizáciu (*International Organization for Standardization*). Je metodikou, ktorá má poskytovať odporúčania pre komplexné riešenie, zavedenie a implementáciu managementu bezpečnosti informačných systémov, a to pre všetky úrovne riadenia organizácie, čím poskytuje pokrytie pre všetky fázy ISMS (*Information Security Management System*).

Vybrané normy ISO/IEC 27000 sú nasledovné:

- **ISO 27000** – poskytuje prehľad systémov riadenia bezpečnosti informácií, zavádza pojmy, definície a slovník termínov pre túto rodinu noriem.
- **ISO 27001** – poskytuje odporúčania o tom, ako aplikovať opatrenia normy ISO 27002. Jedná sa teda o normu stanovujúcu spôsob, ako uplatniť požiadavky systému managementu bezpečnosti informácií.

- **ISO 27002** – poskytuje praktické odporúčania najlepších bezpečnostných praktík a opatrení v oblasti informačnej bezpečnosti.
- **ISO 27003** – poskytuje odporúčania pre ustanovenie a implementáciu systému riadenia bezpečnosti informácií (ISMS) v súlade s radom noriem ISO/IEC 27000.
- **ISO 27799 –** špecifikuje zásady implementácie normy ISO/IEC 27002 v kontexte zdravotníckej informatiky. Zavedením normy ISO/IEC 27002 a ISO/IEC 27799 budú zdravotnícke zariadenia schopné zaistiť minimálnu úroveň zabezpečenia osobných zdravotných informácií pacientov.

Pre malé organizácie, akými sú aj malé zdravotnícke zariadenia, môže byť komplikované aplikovať tieto normy do praxe, či už kvôli technickej a organizačnej náročnosti, finančnej nákladovosti, alebo kvôli rozsiahlej dokumentácii. Normy tvoria odporúčané postupy, a preto organizácia, ktorá sa rozhodne riešiť problematiku informačnej bezpečnosti, nemusí prijať všetky odporúčania, ale môže zvoliť len tie postupy, ktoré sú vyhovujúce pre jej aktuálny stav pri akceptovateľnom finančnom zaťažení a dodržaní vhodného a adekvátneho zabezpečenia, ktoré je vyžadované zákonom.

2.3.1.1. ČSN ISO/IEC 27001:2014

Táto norma je českým prekladom pôvodnej anglickej verzie normy ISO/IEC 27001, ktorej prijatie a preklad zabezpečuje *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví*. Obsahom tejto medzinárodnej normy je špecifikácia požiadaviek na vytvorenie, zavádzanie, údržbu, monitorovanie a neustále zlepšovanie systému riadenia informačnej bezpečnosti organizácie, ako aj špecifikácia požiadaviek na posúdenie a ošetrenie rizík informačnej bezpečnosti v organizácii. Požiadavky, ktoré poskytuje táto norma sú všeobecné a uplatniteľné pre všetky typy organizácií.

Norma je členená na osem kapitol a jej súčasťou sú aj tri prílohy. Prvá príloha stanovuje ciele riadenia a opatrenia, ktoré má spoločnosť dodržiavať a prijať. Druhá popisuje princípy OECD v súvislosti s touto normou a tretia popisuje súvislosti s normami ISO/IEC 9001 a ISO/IEC 14001.

Táto norma klasifikuje 14 oblastí, v ktorých je 35 kategórií a 114 opatrení pre dosahovanie informačnej bezpečnosti.

Tabuľka č. 1: Oblasti riešenia informačnej bezpečnosti podľa normy ČSN ISO/IEC 27001

(Zdroj: Vlastné spracovanie podľa: 8)

ČSN ISO/IEC 27001:2014	Kategórie	Opatrenia
Politiky bezpečnosti informácií	1	2
Organizácia bezpečnosti informácií	2	5-2
Bezpečnosť ľudských zdrojov	3	2-3-1
Riadenie aktív	3	4-3-3
Riadenie prístupu	4	2-6-1-5
Kryptografia	1	2
Fyzická bezpečnosť a bezpečnosť prostredia	2	6-9
Bezpečnosť prevádzky	7	4-1-1-4-1-2-1
Bezpečnosť komunikácií	2	3-4
Akvizície, vývoj a údržba systémov	3	3-9-1
Dodávateľské vzťahy	2	3-2
Riadenie incidentov bezpečnosti informácií	1	7
Aspekty riadenia kontinuity činností organizácie	2	3-1
Súlad s požiadavkami	2	5-3

Táto norma stanovuje minimálny rozsah oblastí, z ktorého vychádza zavádzanie bezpečnosti informácií. Každá organizácia však musí zvážiť relevantnosť daných oblastí pred samotným zavedením opatrení. Je potrebné brať normu ako návod obsahujúci najlepšie možné riešenia v rozoberaných oblastiach.

2.3.2. Vybrané zákony upravujúce bezpečnosť informácií

Slovenská republika má množstvo zákonov, ktoré upravujú zaobchádzanie s informáciami. V problematike zdravotníctva sa zákony orientujú predovšetkým na narábanie, prístup a ochranu citlivých osobných údajov. Zákonov, ktoré sa zaoberajú danou problematikou existuje pre potreby tejto práce veľké množstvo, preto zmienim len niekoľko vybraných.

Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Zákon o ochrane osobných údajov upravuje ochranu práv osôb pred neoprávneným spracovaním osobných údajov a tiež upravuje práva a povinnosti pri spracúvaní takýchto údajov. Zákon vychádza z predpokladu, že prevádzkovateľ, ktorý spracováva osobné údaje, má navrhnutú primeranú ochranu týchto údajov, a to prijatím primeraných technických a organizačných opatrení.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Zákon upravuje bezpečnosť informácií, informačných systémov a sietí, definuje základné požiadavky na zabezpečenie informačných systémov, upravuje konkrétne požiadavky na technické a organizačné opatrenia a stanovuje sankcie za porušenie povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti.

Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti

Keďže osobné údaje o zdravotnom stave pacienta spadajú do osobitnej kategórie osobných údajov, podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov pre tieto údaje platí zákaz spracovania. Podľa zákona č. 576/2004 Z. z. o zdravotnej starostlivosti však tieto údaje možno spracovať za účelom poskytnutia zdravotnej starostlivosti a za účelom plnenia verejného zdravotného poistenia, pričom sa nevyžaduje súhlas od pacienta (čo platí aj pri poskytovaní a sprístupňovaní údajov v špecifických prípadoch).

Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov

Zákon upravuje používanie elektronického podpisu, bezpečnostné pravidlá, práva a povinnosti, ako aj hodnovernosť a ochranu elektronických dokumentov.

Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov

Zákon upravuje pravidlá a princípy zaobchádzania s archívnymi dokumentami v informačných systémoch, ich ochranu a rovnako aj sprístupňovanie týchto dokumentov.

2.4. Systém managementu bezpečnosti informácií ISMS

Systém managementu bezpečnosti informácií ISMS je súčasťou celkového systému managementu organizácie, ktorého cieľom je riadenie bezpečnosti ICT v zmysle ustanovenia, zavedenia, prevádzky, preskúmavania a zlepšovania bezpečnosti informácií v organizácii. Vďaka neustále sa meniacim podmienkam, či už v oblasti vyhodnocovania rizík, alebo iných zmien vnútorného a vonkajšieho okolia organizácie, je zavedenie ISMS dlhodobým a kontinuálnym procesom, ktorý si vyžaduje okamžité reakcie na dané zmeny (1).

Vzhľadom na veľkosť a štruktúru malých zdravotníckych zariadení nie je potrebné, aby sme brali do úvahy všetky odporúčania, ktoré stanovuje norma, ale sústredíme sa len na tie, ktoré sú spoločné a relevantné pre organizácie zaoberajúce sa týmto druhom činnosti. V ďalších odstavcoch tejto kapitoly budú ako teoretický podklad použité normy ČSN ISO/IEC 27000, ČSN ISO/IEC 27001 a ČSN ISO/IEC 27002.

2.4.1. Všeobecné požiadavky a Demingov model PDCA

Pri vedení ISMS v organizácii je nutné spĺňať nasledujúce požiadavky:

- Ustanovenie
- Zavedenie
- Prevádzka
- Monitoring
- Preskúmavanie
- Udržovanie
- Sústavné zlepšovanie

Použitý proces a základný princíp, ktorý využíva ISO pri implementácii ISMS v podnikovom prostredí, vychádza z Demingovho cyklu PDCA (*Plan, Do, Check, Act*), ktorý je aplikovaný na riadenie rizík (1).

Tento model tvoria 4 etapy:

1. **Plánuj (ustanovenie ISMS**): tvorí etapu plánovania, ustanovenia ISMS, definovanie rozsahu a hraníc, definovanie cieľov, postupov a procesov pri riadení informačnej bezpečnosti. Vytvára sa analýza rizík a pripravuje sa plán bezpečnostných opatrení,
2. **Vykonaj (zavedenie a prevádzka ISMS)**: ďalšia etapa zavádza prijaté postupy, definované ciele a procesy riadenia informačnej bezpečnosti do platnosti,
3. **Kontroluj (monitoring a preskúmavanie ISMS)**: v tejto etape nasleduje monitorovanie a meranie výkonu už zavedených a vykonaných opatrení a hlásenie zistených odchýlok vedeniu pre preskúmanie adekvátnosti zavedených postupov ISMS,
4. **Jednaj (udržiavanie a sústavné zlepšovanie ISMS)**: na základe zistených odchýlok a problémov v tretej etape, dochádza v tejto fáze k náprave a stanoveniu nových bezpečnostných opatrení a zmenách za účelom udržiavania neustáleho skvalitňovania ISMS (1).

2.4.2. Ustanovenie ISMS

Proces ustanovenia a riadenia ISMS môžeme zhrnúť do nasledovných krokov:

- vymedzenie hraníc a rozsahu v uplatňovaní ISMS. Vedenie na základe činnosti spoločnosti, aktív, technológií a iných aspektov, rozhodne o potrebnom rozsahu a hraniciach ISMS,
- vytvorenie prehlásenia o politike ISMS, ktorá vzniká na základe charakteristík spoločnosti, štruktúry, činnosti, stavu aktív spoločnosti a iných aspektoch. Politika ISMS upresňuje ciele v oblasti bezpečnosti informácií, ako aj rámec riadenia bezpečnosti informácií s nadväznosťou na legislatívne požiadavky. Politika ISMS musí byť schválená vedením spoločnosti,
- stanovenie metodiky hodnotenia rizík v organizácii, teda stanovenie postupu ako sa budú hodnotiť aktíva v rozsahu stanovenom ISMS, určenie zraniteľností a možných dopadov pre organizáciu. Stanovenie postupu vyhodnocovania rizík a identifikácie variantov ošetrenia rizík,

- odsúhlasenie návrhu bezpečnostných opatrení pre zníženie bezpečnostných rizík, vychádzajúceho z analýzy rizík a posúdenie a akceptácia zvyškových rizík,
- odsúhlasenie dokumentu Prehlásenie o aplikovateľnosti, ktorým spoločnosť ustanoví ciele opatrení, ako aj jednotlivé bezpečnostné opatrenia v rámci ISMS organizácie (4).

2.4.3. Zavedenie a prevádzka ISMS

V tejto etape sa zavádzajú požiadavky prvej etapy tak, ako boli vymedzené. Behom tejto časti by mali byť splnené nasledovné činnosti:

- na základe zostaveného hodnotenia rizík z predchádzajúcej etapy, vytvoriť Plán pre zvládanie rizík a zaviesť ho do prevádzky,
- zaviesť plánované bezpečnostné opatrenia vymedzené ISMS a vytvoriť Príručku bezpečnosti informácií,
- vytvoriť program školení o bezpečnosti informácií pre zamestnancov,
- vytvoriť metriky účinnosti opatrení a monitorovať ich,
- vytvoriť zoznam riešení a postupov pre detekciu a reakciu na bezpečnostné incidenty,
- definovať pravidlá pre dokumentáciu a záznamy ISMS (4).

2.4.4. Monitoring a preskúmavanie ISMS

Cieľom tejto etapy je efektívne monitorovanie a spätná väzba. Pre splnenie tejto časti ISMS je nutné:

- zaviesť systém monitorovania a merania a použiteľných metód monitorovania pre efektívne hodnotenie zavedených opatrení,
- pravidelne vykonávať interné audity a preskúmavať systém ISMS z hľadiska efektivity, vhodnosti a primeranosti,
- pripravovať správy o stave ISMS (4).

2.4.5. Udržiavanie a zlepšovanie ISMS

Za účelom zlepšovania a udržiavania požiadaviek definovaných ISMS je v tejto etape potrebné prijať nasledujúce kroky:

- pri výskyte nezhody je potrebné reagovať a prijať opatrenia k jej náprave, a rovnako prijať opatrenia pre odstránenie príčin nezhody,
- neustále zlepšovať adekvátnosť, vhodnosť a efektivitu systému riadenia bezpečnosti informácií a snažiť sa o dosahovanie stanovených cieľov bezpečnosti informácií (4).

3. ANALÝZA SÚČASNÉHO STAVU

Pre zanalyzovanie súčasného stavu bezpečnosti v zdravotníckych zariadeniach som sa rozhodla vytvoriť dotazník zohľadňujúci aspekty bezpečnosti, ktorými sú fyzická a organizačná bezpečnosť, personálna bezpečnosť, bezpečnosť automatizovaného informačného systému a rovnako tak neautomatizovaného dokumentačného systému. Respondenti odpovedali na 38 otázok. Prieskum bol vykonaný medzi 43 lekármi na celom území Slovenskej republiky, takže respondenti pochádzajú z rôznych miest. Špecializácie týchto lekárov sú rovnako rôznorodé, pričom v najväčšom zastúpení je všeobecné lekárstvo pre dospelých (37,2%), ďalej gynekológia (13,9%), interné lekárstvo (11,6%), pediatria (9,3%), stomatológia (6,9%) a psychiatria (6,9%), ortopédia (4,6%) a napokon v rovnakom percentuálnom zastúpení odbornosti: chirurgia, urológia, rehabilitácia a neurológia (2,3%). Pri analýze budem využívať aj svoje poznatky a analýzy z praxe.

3.1. Zdravotnícke zariadenie

Pre analýzu boli náhodne oslovení lekári, ktorí pracujú v tzv. malých zdravotníckych zariadeniach. Takéto zariadenia je nutné pre potreby tejto práce definovať. Jedná sa o poskytovateľa zdravotnej starostlivosti v ambulantnom zdravotníckom zariadení. V praxi personálne zabezpečenie ambulantného zariadenia tvoria jeden lekár a jedna sestra. Podľa zamerania lekárov rozlišujeme ambulancie prvého kontaktu (všeobecné lekárstvo pre dospelých, všeobecné lekárstvo pre deti a dorast, gynekológia) a ambulancie špecialistov. Tieto sa sústreďujú na prevenciu, diagnostiku a liečbu ochorení s následnou špecializovanou starostlivosťou. Na výkon svojho povolania je nutné dodržať zvláštne požiadavky, aby boli chránené poskytnuté zdravotné informácie subjektov zdravotnej starostlivosti. V týchto zariadeniach však nebýva zvykom, aby bola informačná bezpečnosť riešená systematickým spôsobom.

3.2. Súčasný stav ambulantných zariadení a ich bezpečnosť

3.2.1. Poloha, usporiadanie priestorov a fyzická bezpečnosť

Ambulantné pracoviská lekárov sa takmer v 42% prípadov nachádzajú v prenajatých priestoroch budovy polikliniky, ďalej sú to priestory iných multifunkčných budov (33%), kde sú ambulancie umiestnené spolu s inými podnikmi administratívneho, obchodného či obytného typu. V menšom percentuálnom zastúpení (19%) sa ambulancie nachádzajú v samostatnej budove, kde celý objekt tvorí jednu ambulanciu. Ambulancie v rodinných domoch vo vlastníctve poskytovateľa zdravotnej starostlivosti sa vyskytli takmer v 5% prípadov. Zo všetkých opýtaných, je až v 86% prípadov priestor ambulancie prenajatý, čo značne limituje dodatočnú snahu zlepšovať fyzickú objektovú bezpečnosť. V 53,5% prípadov sa zdravotnícke zariadenie nachádza na prízemí, v menšom zastúpení na prvom poschodí budovy (37,2%), pričom u polovice respondentov existuje voľný prístup k oknám z verejného priestranstva.

Priemerne pozostávajú priestory ambulancií z troch miestností, so štandardným rozložením jednej miestnosti pre lekára, jednej miestnosti pre sestru a samostatnej alebo spoločnej čakárne. Len výnimočne majú lekári k dispozícii ďalšie priestory, akými sú technická, denná, či administratívna miestnosť, prípadne archív (18,6% prípadov). V 70% prípadov je usporiadanie miestností v ambulanciách tvorené viacerými prepojenými miestnosťami, do ktorých je prístup len z hlavných dverí z čakárne.

Nakoľko sa predmetné zariadenia nachádzajú najmä v prenajatých priestoroch polikliník a multifunkčných budov, je zabezpečenie týchto objektov vecou ich prenajímateľov. V 70% prípadov sú objekty v noci uzamknuté a nestrážené. Takmer polovica budov je však vybavená alarmom, ktorý je v 25% prípadov napojený aj na policajné zložky. Zabezpečenie ochrany kamerovým systémom vonkajších priestorov budovy je pomerne zriedkavé (len 9,3% prípadov). Kamerové systémy sa však v malej miere nachádzajú aj vo vnútorných priestoroch. Jedná sa o čakárne, kde tieto zariadenia slúžia predovšetkým na monitoring pacientov (v snahe vylúčenia ohrozenia zdravotného stavu) a neuchovávajú záznamy.

Zabezpečenie objektov prostredníctvom strážnej služby alebo čipových kariet je minimálne (4,65% respondentov v oboch prípadoch). Je nutné podotknúť, že objekty sú

neustále vystavované náporu veľkého množstva pacientov či iných ľudí, nakoľko je až 70% budov verejných. Prítomnosť verejnosti v priestoroch ambulancie vzhľadom k povahe zdravotníckej činnosti nemôže byť nikdy vylúčená.

Priestory ambulancií sú štandardne mechanicky zabezpečené uzamykateľnými dverami, prípadne bezpečnostnými dverami (20,93% prípadov), či dodatočným počtom bezpečnostných zámkov na dverách. Keďže sa väčšina týchto zariadení nachádza na prízemí, či prvom poschodí, kde existuje potenciál zvýšeného prístupu verejnosti k oknám zariadenia, je tento problém v niekoľkých prípadoch zmiernený použitím mreží na oknách (16,28%) alebo bezpečnostných fólií (7%). Priestory ambulancie vybavené alarmom má 35% respondentov. V oblasti so zvýšenou kriminalitou sa nachádza 16,2% opýtaných, napriek tomu u týchto respondentov neexistuje korelácia medzi týmto faktom a zvýšeným fyzickým a mechanickým zabezpečením.

Priestory zdravotníckych zariadení sú vybavené protipožiarnymi bezpečnostnými prvkami. Najvyššie zastúpenie majú hasiace prístroje, hydranty (44,2%) a požiarna signalizácia (42%). V ambulanciách sú tiež povinne vykonávané pravidelné protipožiarne bezpečnostné kontroly.

Jedným z opatrení na zmiernenie následkov narušenia bezpečnosti je aj poistenie ambulancie. V tomto prípade je 53,5% respondentov poistených, pričom v najvyššej miere je to poistenie proti krádeži majetku. Ďalej je to poistenie voči živelnej pohrome, vandalizmu, či poistenie voči škodám pri výkone povolania.

Medzi fyzickú bezpečnosť patrí aj umiestnenie zariadení. Vzhľadom na priestorové obmedzenie ambulancií by mali pracovné stanice s osobnými zdravotnými informáciami byť umiestnené tak, aby nedochádzalo k priamemu vizuálnemu kontaktu s obrazovkou počítača. V 16,3% prípadov však pacienti priamo vidia obrazovky pracovných staníc.

3.2.2. Personálne zastúpenie a bezpečnosť

Ako už bolo spomenuté, malé zdravotnícke zariadenie je charakteristické práve tým, že má limitovaný počet zamestnancov. Zväčša sa jedná o jedného lekára a sestru, nie je to však pravidlom. Zriedkavo počet zamestnaných lekárov prekračuje jednu osobu, ide však len o výnimky (2% prípadov). Počet ostatného zdravotníckeho personálu, ktorý tvoria sestry, je o niečo vyšší. Štandardom je však opäť jedna sestra (88,4%), výnimočne sú to

dve sestry (9,3%) a len v zariadeniach, akými sú rehabilitačné ambulancie, je počet sestier mnohonásobne vyšší (2,3%), v prípade respondenta išlo o 7 sestier.

Súčasťou týchto zariadení je aj nezdravotnícky personál. Jedná sa predovšetkým o pomocný personál, upratovačky, ekonómky či personál zabezpečujúci administratívu. 56% respondentov uvádza, že má jedného takéhoto zamestnanca, u 14% respondentov sú to dvaja zamestnanci. Títo však nie sú zamestnancami na plný úväzok, ale pracujú na dohodu a okrem pracovníkov poskytujúcich upratovacie služby, pracujú externe.

S informačným systémom a zdravotníckymi údajmi pracujú priemerne dvaja ľudia, lekár a sestra, tento počet sa samozrejme zvyšuje s pribúdajúcim zdravotníckym personálom. Pri spracovaní dávkových súborov do poisťovní sa ale s týmito dátami môžu stretávať osoby, ktoré ich spracúvajú, ak to nevykonáva sám lekár (9,3% prípadov).

3.2.3. Infraštruktúra ICT a komunikačná a softvérová bezpečnosť

Infraštruktúra je zabezpečovaná externými dodávateľmi, nakoľko väčšina poskytovateľov zdravotnej starostlivosti sídli v prenajatých priestoroch, zabezpečuje ju zväčša prenajímateľ. V prípade súkromných ambulancií sídliacich v poliklinikách, prenajímateľ rovnako zabezpečuje služby poskytovateľa internetu ako aj telefónu, takže v priestoroch ambulantných zariadení zamestnanci zodpovedajú len za pracovné prepojenie staníc od zásuviek, prípadne za aktívne prvky, ak sú umiestnené na pracovisku a sú v priamom vlastníctve nájomcu (vlastný router má len 30% respondentov). Technik, ktorého zamestnáva prenajímateľ, nezodpovedá za funkčnosť infraštruktúry v prenajatých priestoroch.

Počet pracovných staníc jednotlivých ambulancií koreluje s počtom zdravotníckeho personálu. Jedna ambulancia má teda priemerne dve pracovné stanice, medzi ktorými je vytvorená sieť. Vlastný samostatný server sa v ambulanciách vyskytuje len sporadicky (2,3% prípadov). Ambulancie využívajú operačné systémy spoločnosti Microsoft, pričom v najväčšom zastúpení sa jedná o Windows 10. V menšom počte sa stále vyskytuje aj Windows 7 Professional (17%) a Windows 8 (3%). Napriek ukončenej podpore pre Windows XP, stále evidujeme na celom trhu aj lekárov, ktorí tento operačný systém napriek tomu používajú, je to však nepatrný počet (0,27%).

Softvérové vybavenie počítačov sa líši. Štandardne však obsahuje kupované licencované programy, predovšetkým ambulantný softvér a editačný softvér. U lekárov, špecialistov, sa vyskytujú aj iné programy, potrebné pre výkon ich činnosti (napr. softvér pre panoramatický röntgen, tlakový holter, EKG), ktoré taktiež zberajú a uchovávajú citlivé údaje pacientov.

Každá pracovná stanica je podľa respondentov vybavená antivírusovým programom, medzi ktorými prevláda riešenie spoločnosti ESET, prípadne vstavaná ochrana operačného systému Windows 10, Defender. Niekoľko poskytovateľov zdravotnej starostlivosti však využíva aj voľne šíriteľné softvérové riešenia.

Zabezpečenie plynulej dodávky elektriny pre pracovné stanice, tzv. nepretržitý zdroj napájania UPS, používa len 25,6% lekárov.

3.2.4. Opatrenia v oblasti bezpečnosti a práca s dátami

Interná organizácia v oblasti bezpečnosti v ambulantných zariadeniach

Malé zdravotnícke zariadenia zväčša nemajú definované role a zodpovednosti za bezpečnosť informácií v žiadnej dokumentovanej forme. Pravidlá bezpečnosti zdravotníckych informácií sú určené predovšetkým na základe *Zákona č. 576/2004 Z. z. o zdravotnej starostlivosti*, podľa ktorého musia chrániť zdravotnú dokumentáciu pacientov pred stratou, zneužitím, poškodením alebo zničením, a rovnako spadajú pod inštitút povinnosti mlčanlivosti. Tieto pravidlá sú samozrejme všeobecne známe, ako aj povinnosť ich dodržiavania, problémom je však určenie spôsobu ako ich dodržiavať.

Posun v tejto oblasti bol zaznamenaný od roku 2013, kedy vznikla zákonná povinnosť mať vypracovaný Bezpečnostný projekt aj pre zdravotnícke zariadenia. Okrem iného, by súčasťou Bezpečnostného projektu mali byť špecifikované práve zodpovednosti za bezpečnosť informácií, ako aj minimálne jedna osoba, ktorá zodpovedá za bezpečnosť zdravotníckych informácií. Určenou zodpovednou osobou je vždy lekár, no z praxe môžem potvrdiť, že túto dokumentáciu považujú lekári len za povinnosť, bez prikladania hlbšieho významu k aplikovaniu pravidiel.

Vzdialený prístup a práca na diaľku

Lekári častokrát využívajú možnosť práce z domu, predovšetkým sa jedná o dodatočné administratívne úkony vykazovania zdravotníckej agendy a čoraz častejší je aj home office. Podľa prieskumu sa 7% lekárov prihlasuje cez vzdialený prístup na svoj počítač v ambulancii[1]. Z prieskumu tiež vyplýva, že osobné údaje pacientov sa nachádzajú aj v počítačoch (30%) a notebookoch (9,3%), ktoré sú umiestnené u lekárov doma.

Systém hesiel

Využitie hesiel pre zaistenie autentifikácie a autorizácie je potrebné ako pri vstupe do operačného systému, tak aj do ambulantného programu. Podľa výsledkov prieskumu až 58% nemá operačný systém chránený heslom. Vstup do operačného systému je chránený heslom, ktoré pozostáva priemerne z dvoch znakov. Ambulantný program je chránený prístupovým heslom, ktoré sa priemerne skladá zo 4 znakov. Bez akéhokoľvek hesla je 14% respondentov. Heslo do ambulantného programu 65% lekárov nemení vôbec. 21% ho mení každého pol roka a 14% raz za rok.

Zálohovanie

V prípade potreby zachovania bezpečnosti zdravotníckych údajov je nutné popísať aj súčasný stav zálohovania týchto dát. Ukazuje sa, že pravidelne si zálohuje svoje dáta 86% lekárov, 14% lekárov svoje dáta zálohuje nepravidelne, alebo vôbec. 63% lekárov pritom zálohuje v časovom intervale jeden deň, 21% zálohuje jeden až dvakrát týždenne a zvyšná časť lekárov zálohuje v rozmedzí dvoch týždňov až piatich mesiacov. Ambulantný program, ktorý obsahuje majoritnú časť zdravotníckych dát, ponúka možnosť úplnej, diferenčnej aj inkrementálnej zálohy na tri médiá naraz (možnosť voľby), pričom existuje možnosť mechanickej alebo automatickej zálohy. Zálohy sú šifrované. Štandardne lekári ukladajú dáta predovšetkým na pevný disk počítačov v sieti a na zvolené externé médium (využívajú hlavne USB alebo externý HDD). Prenosné zálohové médiá sa nachádzajú zväčša uzamknuté (35%) alebo neuzamknuté v ambulancii (11,6%), prípadne ich lekári nosia stále pri sebe (28%). Až polovica opýtaných tieto

[1] Pozn. toto číslo je v súčasnej kríze koronavírusu niekoľkonásobne vyššie, nakoľko mnoho lekárov ambuluje z domu a vyšetruje pacientov dištančne.

médiá prenáša domov, alebo zálohuje dáta na notebook, ktorý prenáša na pracovisko a domov.

Likvidácia dát

Dáta uložené na pevných diskoch pracovných staníc a dáta uložené na výmenných médiách musia podliehať pravidlám bezpečnej likvidácie. Prieskum ukázal, že 58% respondentov vymazáva dáta z média bežným spôsobom. Špeciálny softvér pre vymazanie dát využíva len 2,3% lekárov, formátovanie média 16,3% a znehodnotenie média 23,3% respondentov.

Riešenie porúch

Pri poruchách počítača alebo softvérových chybách, lekári odovzdávajú počítače do špecializovaného servisu v 26% prípadov, záleží však od charakteru poruchy. Zvyčajne však technik prichádza priamo na pracovisko ambulancie. O odbornosti práce sa dá v tomto prípade polemizovať, častokrát sú to rodinní príslušníci, priatelia, alebo sami lekári.

Likvidácia dát dokumentačne spracovaného IS

Všetci lekári musia zo zákona viesť zdravotnú dokumentáciu pacientov aj v písomnej podobe. Tieto záznamy musia byť uložené v uzamykateľných zásuvkových kartotékach alebo skriniach. Niektorí lekári vedú aj ambulantnú knihu, knihu práceneschopných, knihu röntgenov, zoznam očkovaných, zoznamy protetických prác a podobné pomocné knihy a účtovné doklady. Napriek faktu, že zásuvkové skrine na dokumenty musia byť uzamykateľné, až 7% respondentov uviedlo, že takéto vybavenie v ambulancii nemá.

Likvidácia dát tlačených dokumentov musí taktiež rešpektovať pravidlá bezpečnej likvidácie. Podľa prieskumu likviduje dokumenty skartovaním 58% lekárov, 7% likviduje dokumenty spaľovaním a 35% lekárov dokumenty vôbec nelikviduje.

3.3. Zhodnotenie súčasného stavu bezpečnosti

Získané údaje o stave informačnej bezpečnosti naznačujú, že aj v prostredí, akým je zdravotnícke zariadenie, nie sú jasne stanovené a dodržiavané pravidlá, ktoré by zabezpečili dostatočnú ochranu osobných zdravotných informácií. Nakoľko je ťažké skĺbiť v osobe lekára aj osobu, ktorá by aktívne zodpovedala a riadila bezpečnosť

informácií, nachádzame aj v tomto priestore niekoľko zásadných problematických miest. Predovšetkým sa jedná o samotné technické vybavenie, ktoré je zväčša nedostatočne zabezpečené, nie sú vykonávané aktualizácie ako operačného systému, tak aj programového vybavenia, čo často vyúsťuje do problémov spojených s nedostupnosťou dát. Rovnako podhodnotená je aj pravidelná kontrola funkčnosti technických zariadení, predovšetkým pevných diskov pracovných staníc. Časté problémy nastávajú aj pri neodbornom zosieťovaní počítačov, pri neodbornom nastavení funkcionalít a pri nedodržiavaní základných princípov bezpečnej práce s počítačom. Predovšetkým systém zabezpečenia prostredníctvom hesiel je alarmujúci, nakoľko až v 58% prípadov nebol operačný systém vôbec zabezpečený heslom. V prípade zabezpečenia ambulantného programu heslom, je toto percento nižšie (14% nemá žiadne heslo), no priemerný počet štyroch znakov hesla u ostatných respondentov je rovnako absolútne nedostatočný. Tento nepriaznivý stav môže viesť k narušeniu komunikačnej bezpečnosti.

Pomerne veľkú časť problémov tvorí systém zálohovania. Lekárom, ktorí zálohujú dáta nepravidelne alebo vôbec, hrozí, že v prípade narušenia bezpečnosti, straty, poškodenia, výmazu údajov či výpadku informačného systému nebudú mať možnosť tieto údaje opätovne obnoviť. S tým sú opäť spojené aj pravidlá zaisťujúce samotný systém zálohovania, ako aj bezpečnú likvidáciu údajov a aj samotných zálohových médií.

Pravidlá rovnako chýbajú i pri práci z domu, práci na diaľku a tiež pre uchovávanie zdravotných dát na počítačoch a médiách umiestnených doma. Pri práci na diaľku sa v praxi často stretávame s problémom neznalosti princípov bezpečnej komunikácie a práce na diaľku, ako aj metód zabezpečenia vzdialeného prístupu. Nakoľko domáce počítače majú spravidla ešte horší systém zabezpečenia ako tie pracovné, existuje pomerne jednoduchá možnosť napadnutia. V týchto prípadoch tiež nie je vylúčené, že sa k dátam dostanú aj rodinní príslušníci, alebo iné osoby.

Z hľadiska personálnej bezpečnosti sa v malých zdravotníckych zariadeniach stretávame predovšetkým s problémom nedostatočnej odbornosti pri bezpečnej práci s dátami, s technickými zariadeniami, ale aj s neznalosťou postupov pri zvládaní bezpečnostných incidentov. K porušeniu bezpečnosti dochádza v týchto prípadoch zväčša neúmyselne, ale definovaním rolí a zodpovedností, ako aj pravidiel a zaškolením osôb, by sa im mohlo dať úplne vyhnúť. Personálne obsadenie ambulancií naznačuje

prípady, kedy sa okrem lekára a sestry vyskytujú v priestoroch ambulancie aj iné osoby, predovšetkým ekonómovia, účtovníci či technici. Mali by preto existovať aj pravidlá zamedzujúce prístup k údajom, pre ktoré tieto osoby nemajú autorizáciu.

Problémom sa zdá byť aj fakt, že väčšina poskytovateľov ambulantnej zdravotnej starostlivosti sídli v prenajatých priestoroch, a teda je limitovaná ako prostredím, tak aj technickými a komunikačnými prostriedkami, ktoré zabezpečuje prenajímateľ. Snahy o dodatočné fyzické zabezpečenie sú teda značne limitované.

Súčasný stav bezpečnosti informácií v zdravotníckych zariadeniach je možné zlepšiť len nastavením pravidiel a vymedzením rolí a zodpovedností. Preto v ďalšej časti tejto práce, na základe analýzy rizík, vytvorím metodický návrh osvedčených postupov a opatrení informačnej bezpečnosti pre malé zdravotnícke zariadenia.

3.4. Analýza rizík

Základnou podmienkou pre vytvorenie osvedčených postupov a opatrení na ochranu informácií je vytvorenie analýzy rizík, pomocou ktorej identifikujeme informačné aktíva a vymedzíme potencionálne hrozby, ktoré na ne môžu vplývať. Identifikované hrozby boli rozdelené z hľadiska úmyslu. V analýze sú aktíva a aj hrozby ohodnotené a sú posúdené možné riziká.

3.4.1. Identifikácia informačných aktív

Všeobecne môžeme v ambulantnom sektore identifikovať informačné aktíva uvedené nižšie v tabuľke 2.

Tabuľka č. 2: Identifikácia informačných aktív

(Zdroj: Vlastné spracovanie)

Informačné aktíva	Databázy ambulantného informačného systému Údajové súbory
Papierová dokumentácia	Zdravotné karty pacientov Ambulantná kniha
Softvérové aktíva	Ambulantný informačný systém Systémový softvér

Fyzické aktíva	Pracovné stanice Externé zálohové médiá Aktívne sieťové prvky + kabeláž Medicínske prístroje (holter, EKG, EEG, röntgen, ultrazvuk,...)
Služby	Výpočtové a komunikačné služby tretích strán

3.4.2. Ohodnotenie informačných aktív

Jednotlivé aktíva musia byť následne ohodnotené. Hodnotu tvorí veľkosť dopadu pri ohrození atribútov bezpečnosti informačných aktív, teda dôvernosti, dostupnosti a integrity. K hodnoteniu bola využitá klasifikačná schéma hodnotenia aktív v tabuľke 3.

Tabuľka č. 3: Klasifikačná schéma hodnotenia aktív

(Zdroj: Vlastné spracovanie)

Dopad / Označenie	Charakteristika dopadu
Žiadny 1	Nedošlo k významnému narušeniu a nie je ovplyvnená funkcionalita aktíva, ani poskytovanie zdravotnej starostlivosti.
Zanedbateľný 2	Nedošlo k porušeniu zákonných požiadaviek. Je možné rýchlo prinavrátiť pôvodný stav aktíva. Dopad sa neprejaví v poskytovaní zdravotnej starostlivosti.
Nízky 3	Mohlo dôjsť k porušeniu zákonných požiadaviek. Dopad sa neprejaví v poskytovaní zdravotnej starostlivosti. Prinavrátenie pôvodného stavu aktíva trvá dlhšie. Mohlo dôjsť k narušeniu bezpečnosti citlivých údajov.
Nežiaduci 4	Vznik vážnych problémov a finančných strát. Vážny dopad na poskytovanie zdravotnej starostlivosti a na funkcionalitu aktíva. Mohlo dôjsť k narušeniu bezpečnosti citlivých údajov.
Neprijateľný 5	Existenčné problémy pre spoločnosť spojené s vážnymi dopadmi na aktívum. Nie je možné poskytovať zdravotnú starostlivosť. Došlo k narušeniu bezpečnosti citlivých údajov.

Nasledujúca tabuľka zobrazuje ohodnotenie informačných aktív. Pri každom aktíve je stanovená hodnota dopadu z hľadiska dôvernosti, dostupnosti a integrity. Stĺpec Hodnota označuje výslednú hodnotu dopadu vypočítanú spriemerovaním predošlých hodnôt.

Tabuľka č. 4: Hodnotenie aktív

(Zdroj: Vlastné spracovanie)

Aktívum	Dopad na			Hodnota
	Dôvernosť	Dostupnosť	Integritu	
Databázy ambulantného IS	5	4	5	5
Údajové súbory	2	1	1	1
Zdravotné karty pacientov	5	3	4	4
Ambulantná kniha	4	1	1	2
Ambulantný IS	5	4	5	5
Systémový softvér	4	3	3	3
Pracovné stanice	4	3	3	3
Externé zálohové médiá	5	4	4	4
Aktívne sieťové prvky + kabeláž	3	3	3	3
Medicínske prístroje	4	3	4	4
Výpočtové a komunikačné služby tretích strán	1	2	2	2

3.4.3. Identifikácia hrozieb a hodnotenie pravdepodobnosti

V prostredí malých zdravotníckych zariadení boli s využitím normy ISO/IEC 27005 a za pomoci odborníka v tejto oblasti identifikované nasledujúce hrozby, ktoré boli ohodnotené podľa toho, s akou pravdepodobnosťou môžu nastať a akú veľkosť dopadu predstavujú. K hodnoteniu bola využitá klasifikačná schéma hodnotenia hrozieb v tabuľke 5.

Tabuľka č. 5: Klasifikačná schéma hodnotenia hrozieb

(Zdroj: Vlastné spracovanie)

Úroveň hrozby	Charakteristika hrozby
1	Pravdepodobnosť, že hrozba nastane je zanedbateľná.
2	S malou pravdepodobnosťou môže dôjsť k uskutočneniu hrozby.
3	Pravdepodobne môže dôjsť k uskutočneniu hrozby.
4	Hrozba môže nastať s pomerne vysokou pravdepodobnosťou.
5	Takmer určite môže dôjsť k uskutočneniu hrozby.

Nasledujúca tabuľka zobrazuje identifikované hrozby a ich hodnotenie.

Tabuľka č. 6: Identifikácia hrozieb a miera pravdepodobnosti

(Zdroj: Vlastné spracovanie)

IČ	Hrozba	Pravdepodobnosť
Náhodné hrozby		
	Prírodné hrozby	
1	Povodeň	2
2	Požiar	2
3	Víchrica	2
4	Iná živelná pohroma	1
	Výpadok služieb	
5	Výpadok elektrickej energie	4
6	Výpadok internetového pripojenia	3
7	Výpadok IS	3
8	Výpadok bezpečnostného systému	2
	Technické zlyhania	
9	Zlyhanie serveru	3
10	Zlyhanie pracovnej stanice	3
11	Zlyhanie častí ICT infraštruktúry	2

12	Zlyhanie medicínskych prístrojov	2
13	Poškodenie dát	3
Úmyselné hrozby		
	Fyzické hrozby	
14	Krádež technického vybavenia	3
15	Krádež médií	3
16	Krádež dokumentov	2
	Iné úmyselné hrozby	
17	Neoprávnený prístup do priestorov	3
18	Neoprávnené získanie prístupových údajov	3
19	Neoprávnené získanie dát	3
20	Zneužitie užívateľského oprávnenia	2
21	Napadnutie ICT	2
22	Napadnutie IS	2
23	Získanie dát z vyradených médií	2
24	Inštalácia škodlivého softvéru	4
25	Zámerné odstraňovanie dát	2
26	Porušenie mlčanlivosti	2
Neúmyselné hrozby		
	Fyzické hrozby	
27	Nehoda na pracovisku s následnými škodami	2
28	Strata médií	3
	Iné neúmyselné hrozby	
29	Chyby personálu pri práci s IS	5
30	Chyby pri nastavení prístupových práv	4
31	Chyby pri správe IT služieb	3
32	Nedbanlivosť pri údržbe zariadení	3
33	Nedodržiavanie predpisov pri práci s informáciami	2

3.4.4. Matica zraniteľnosti

Vytvoríme maticu zraniteľnosti identifikovaných informačných aktív s použitím hodnôt aktív a pravdepodobnosťami hrozieb stanovenými v predchádzajúcich podkapitolách. Zraniteľnosti určíme prostredníctvom klasifikačnej schémy v tabuľke č. 7.

Tabuľka č. 7: Klasifikačná schéma zraniteľností aktív

(Zdroj: Vlastné spracovanie)

Hodnota	Charakteristika zraniteľnosti
1	Zanedbateľná zraniteľnosť
2	Mierna zraniteľnosť
3	Stredná zraniteľnosť
4	Vysoká zraniteľnosť
5	Veľmi vysoká zraniteľnosť

Tabuľka č. 8: Matica zraniteľnosti

(Zdroj: Vlastné spracovanie)

	Pravdepodobnosť	Databázy ambulantného IS	Údajové súbory	Zdravotné karty pacientov	Ambulantná kniha	Ambulantný IS	Systémový softvér	Pracovné stanice	Externé zálohové médiá	Aktívne sieťové prvky + kabeláž	Medicínske prístroje	Výpočtové a komunikačné služby
Hodnota aktíva		5	1	4	2	5	3	3	4	3	4	2
Povodeň	2	2	2	4	4	2	2	4		3	4	
Požiar	2	2	2	4	4	2	2	4		4	4	
Víchrica	2							1		1	1	2
Iná živelná pohroma	1			1	1			2		2	3	3
Výpadok elektrickej energie	4	3	1			3	2	4		2	4	5
Výpadok internetového pripojenia	3					2					2	5
Výpadok IS	3	4	1			5	5	1		1	2	
Výpadok bezpečnostného systému	2	1	1	3	3	2	2	4	2	3	4	
Zlyhanie serveru	3	4	4			2	2	5		2	1	1
Zlyhanie pracovnej stanice	3	1	1			1	2	5			1	
Zlyhanie častí ICT infraštruktúry	2	3	2			3	1	3		5	2	4
Zlyhanie medicínskych prístrojov	2	1	1								5	
Poškodenie dát	3	4	3			1	1	1	4			
Krádež technického vybavenia	3	4	4			2	3	5		5	5	1

Krádež médií	3	2	2			1			5			
Krádež dokumentov	2			5	5							
Neoprávnený prístup do priestorov	3	1	1	3	2	1	1	3	3	1	2	
Neoprávnené získanie prístupových údajov	3	1	1			4	4	4	2	3		
Neoprávnené získanie dát	3	2	2	3	2	2			4		2	
Zneužitie užívateľského oprávnenia	2	4	4	4	4	3	3		1	1		
Napadnutie ICT	2	4	4			4	4	4		5	4	
Napadnutie IS	2	5	5			5	4	3		2	4	
Získanie dát z vyradených médií	2	3	3						4			
Inštalácia škodlivého softvéru	4	5	5			1	4	2	1	3	3	
Zámerné odstraňovanie dát	2	5	4	5	3	4			5		2	
Porušenie mlčanlivosti	2	2	1	5	4	3						
Nehoda na pracovisku s následnými škodami	2	1	1	3	3	1	1	3	1	2	3	
Strata médií	3	2	2			1			5			
Chyby personálu pri práci s IS	5	4	2	2	1	3	1	1			2	
Chyby pri nastavení prístupových práv	4	3	2			2	3	1	1	4	1	2
Chyby pri správe IT služieb	3	2	1			1	2	2	1	3	1	1
Nedbanlivosť pri údržbe zariadení	3	4	4			3	3	4	2	2	3	
Nedodržiavanie predpisov pri práci s informáciami	2	3	2	2	1	2	1		2		2	

3.4.5. Výpočet miery rizika

Mieru rizika stanovíme na základe vzorca *R = T*A*V*,

kde, *R = miera rizika,*

T = pravdepodobnosť vzniku hrozby,

A = hodnota aktíva,

V = zraniteľnosť aktíva.

Miera rizika umožňuje vyjadriť dôležitosť, s akou budeme tvoriť bezpečnostné opatrenia. Jednotlivé miery rizík boli klasifikované podľa tabuľky č. 9.

Tabuľka č. 9: Klasifikačná schéma miery rizika

(Zdroj: Vlastné spracovanie)

Hranica rizika	Miera rizika	Manipulácia s rizikom
0 - 9	Bezvýznamné riziko	akceptácia
10 - 19	Akceptovateľné riziko	akceptácia
20 - 29	Mierne riziko	riešenie rizika
30 - 59	Nežiaduce riziko	riešenie rizika s prioritou
60 a viac	Neprijateľné riziko	riešenie rizika s najvyššou prioritou

Tabuľka č. 10: Matica rizík

(Zdroj: Vlastné spracovanie)

	Databázy ambulantného IS	Údajové súbory	Zdravotné karty pacientov	Ambulantná kniha	Ambulantný IS	Systémový softvér	Pracovné stanice	Externé zálohové médiá	Aktívne sieťové prvky + kabeláž	Medicínske prístroje	Výpočtové a komunikačné služby
Povodeň	20	4	32	16	20	12	24		18	32	
Požiar	20	4	32	16	20	12	24		24	32	
Víchrica							6		6	8	8
Iná živelná pohroma			4	2			6		6	12	6
Výpadok elektrickej energie	60	4			60	24	48		24	64	40
Výpadok internetového pripojenia					30					24	30
Výpadok IS	60	3			75	45	9		9	24	
Výpadok bezpečnostného systému	10	2	24	12	20	12	24	16	18	32	
Zlyhanie serveru	60	12			30	18	45		18	12	6
Zlyhanie pracovnej stanice	15	3			15	18	45			12	
Zlyhanie častí ICT infraštruktúry	30	4			30	6	18		30	16	16
Zlyhanie medicínskych prístrojov	10	2								40	
Poškodenie dát	60	9			15	9	9	48			
Krádež technického vybavenia	60	12			30	27	45		45	60	6

Krádež médií	30	6			15			60			
Krádež dokumentov			40	20							
Neoprávnený prístup do priestorov	15	3	36	12	15	9	27	36	9	24	
Neoprávnené získanie prístupových údajov	15	3			60	36	36	24	27		
Neoprávnené získanie dát	30	6	36	12	30			48		24	
Zneužitie užívateľského oprávnenia	40	8	32	16	30	18		8	6		
Napadnutie ICT	40	8			40	24	24		30	32	
Napadnutie IS	50	10			50	24	18		12	32	
Získanie dát z vyradených médií	30	6						32			
Inštalácia škodlivého softvéru	100	20			20	48	24	16	36	48	
Zámerné odstraňovanie dát	50	8	40	12	40			40		16	
Porušenie mlčanlivosti	20	2	40	16	30						
Nehoda na pracovisku s následnými škodami	10	2	24	12	10	6	18	8	12	24	
Strata médií	30	6			15			60			
Chyby personálu pri práci s IS	100	10	40	10	75	15	15			40	
Chyby pri nastavení prístupových práv	60	8			40	36	12	16	48	16	16
Chyby pri správe IT služieb	30	3			15	18	18	12	27	12	6
Nedbanlivosť pri údržbe zariadení	60	12			45	27	36	24	18	36	
Nedodržiavanie predpisov pri práci s informáciami	30	4	16	4	20	6		16		16	

3.4.6. Vyhodnotenie výsledkov analýzy rizík

Bolo identifikovaných 17 rizík s neprijateľnou úrovňou, a preto by mali byť ošetrené s najvyššou prioritou. Z matice rizík vyplýva, že medzi najohrozenejšie aktíva patria databázy ambulantného IS, ambulantný IS, externé zálohové médiá a medicínske prístroje. Jedná sa predovšetkým o aktíva, ktoré sú cenené vzhľadom k obsahu osobných zdravotných informácií a o medicínske prístroje, ktoré môžu byť tiež citlivé na osobné údaje a zároveň sú aj finančne vysoko cenené. V prípade narušenia bezpečnosti niektorého z týchto aktív hrozia legálne aj finančné škody. Medzi najväčšie hrozby patrí inštalácia škodlivého softvéru, chyby personálu pri práci s IS, výpadok IS a výpadok elektrickej energie. Ďalej je to krádež technického vybavenia, krádež a strata médií, zlyhanie serveru a poškodenie dát. Problematickými sú aj hrozby spojené s chybami pri nastavovaní prístupových údajov a ich neoprávneným získaním a s nedbanlivosťou pri údržbe zariadení. V ďalšej časti práce budeme postupovať tak, aby boli zavedené opatrenia, ktoré budú modifikovať práve riziká s neprijateľnou a nežiaducou mierou u stanovených aktív a hrozieb.

4. VLASTNÉ NÁVRHY RIEŠENIA

V tejto kapitole sú navrhnuté konkrétne opatrenia proti rizikám, ktoré by mali prijať ambulantné zdravotnícke zariadenia pre zvýšenie bezpečnosti informácií, a ktoré rovnako povedú k zavedeniu vybraných častí normy ISO/IEC 27001 a ISO/IEC 27002 v prípade, že by sa takéto zariadenia rozhodli zaviesť ISMS. Spracované opatrenia sú pre ľahšiu orientáciu zoradené a pomenované rovnako, ako jednotlivé kapitoly a podkapitoly normy ISO/IEC 27002. Pri návrhu týchto opatrení vychádzam z normy ISO/IEC 27002 doplnenú normou ISO/IEC 27799.

4.1. Návrh opatrení

4.1.1. A.6 Organizácia bezpečnosti informácií

A.6.1.1 Role a zodpovednosti bezpečnosti informácií

Opatrenie:

Musia byť definované zodpovednosti v oblasti bezpečnosti informácií v súlade s politikou informačnej bezpečnosti organizácie. Zodpovednosti jednotlivých zamestnancov budú definované v pracovných zmluvách.

Za dodržiavanie definovaných postupov a opatrení, ako aj za bezpečnosť osobných zdravotných informácií bude zodpovedať formálne prehlásená zodpovedná osoba, ktorou je lekár, pokiaľ nebude stanovené inak, alebo iná osoba, na ktorú budú delegované povinnosti správy IT.

Zamestnanci budú raz ročne zaškolení predmetom smerníc, za čo bude zodpovedať zodpovedná osoba, alebo iná osoba s delegovanými právami z externej organizácie. Každý rok bude vykonávaná kontrola zamestnancov z dodržiavania smerníc. Noví zamestnanci budú povinne zaškolení predmetom smerníc a zaškolení pre prácu s ambulantným softvérom, s osobnými údajmi a technickými prostriedkami. Povinnosť absolvovať školenie bude stanovená v pracovnej zmluve.

Práva a povinnosti zamestnancov v oblasti dodržiavania opatrení, ako aj sankcie plynúce z ich nedodržania budú definované v pracovných zmluvách tak, aby boli v súlade s politikou informačnej bezpečnosti.

Odporučenie:

- Osoba zodpovedajúca za bezpečnosť informácií je lekár, ktorému patrí ambulancia, prípadne lekár, ktorého najíma VÚC, pokiaľ nebude stanovené inak, alebo iná osoba, na ktorú budú delegované povinnosti správy IT.
- Zodpovedná osoba zodpovedá za pravidelné školenie a oboznámenie personálu s politikami a pravidlami.
- Za bezpečnosť aktív používaných v ambulancii zodpovedajú všetci zamestnanci zdravotníckeho zariadenia.
- Zamestnanci sú povinní dodržiavať stanovené opatrenia, bezpečnostné smernice a postupy, pričom táto povinnosť musí vychádzať z ich zmluvného vzťahu. Rovnako majú povinnosť monitorovať zraniteľnosti aktív a nahlasovať bezpečnostné udalosti a incidenty, ako aj zistenie porušenia stanovených pravidiel zodpovednej osobe.
- Na prácu s osobnými zdravotnými informáciami a informačnými systémami sú oprávnení len lekári a sestry, z čoho vyplýva povinnosť zamedziť tretím osobám prístup k týmto informáciám a systémom.
- V prípadoch, kedy je nevyhnutný prístup do priestorov ambulancie (okrem subjektu zdravotnej starostlivosti), alebo k informačnému systému tretím osobám (predovšetkým tým, ktoré poskytujú ambulancii ďalšie služby ako účtovníctvo a externá správa IT), je potrebné s nimi uzavrieť pracovnú zmluvu, ktorej súčasťou bude poučenie osoby o práci s citlivými osobnými údajmi. V týchto prípadoch je tiež pri práci s informačnými systémami potrebné dodržať pravidlo komisionálnosti.

A.6.2.1 Politika mobilných zariadení

Opatrenie:

Pravidlá používania mobilných zariadení budú definované v smernici o mobilných zariadeniach. V tejto smernici musia byť zadefinované riziká spojené s používaním mobilných zariadení v prostredí ambulancie a preventívne opatrenia a obmedzenia pre

používanie súkromných aj pracovných mobilných zariadení. Dodržiavanie smernice o mobilných zariadeniach bude zakotvené v pracovnej zmluve.

Odporučenie:

- Je zakázané BYOD (*Bring Your Own Device*), teda využívanie zariadení vo vlastníctve zamestnancov, ak nie sú zabezpečené podľa pokynov.
- Je zakázané pripájať sa mobilnými zariadeniami do vnútornej siete.
- Je zakázané pripájať mobilné zariadenia k pracovným staniciam.
- Je zakázané zálohovať údaje, alebo nahrávať údaje na mobilné zariadenia.
- Mobilné zariadenia musia mať nainštalovaný antivírusový softvér a musia byť pravidelne aktualizované.
- Je zakázané, aby sa subjekty zdravotnej starostlivosti pripájali mobilnými zariadeniami na bezdrôtovú sieť ambulancie, pokiaľ neexistuje vyhradená bezdrôtová sieť pre verejnosť.

A.6.2.2 Práca na diaľku

Opatrenie:

Opatrenia, podmienky a obmedzenia pre dodržanie bezpečnosti informácií v miestach, kde sa pracuje na diaľku, budú definované v smernici o práci na diaľku. Rovnako budú definované preventívne opatrenia pre prácu na diaľku a dodržiavanie smernice bude zakotvené v pracovnej zmluve.

Odporučenie:

- Pri práci na diaľku z domu musí byť domáca sieť zabezpečená, preto je potrebné nastaviť na routri alebo access pointe dostatočne silné administrátorské heslo a rovnako zabezpečiť dostatočne silným heslom pripojenie na zariadenie.
- Pre zabezpečenie bezdrôtovej siete musí byť použitý protokol WPA2 alebo WPA3.
- Musí sa zaistiť nastavenie prístupnosti priečinkov zdieľaných cez sieť len pre presne definovaných používateľov.
- Operačný systém počítača, na ktorom sa vzdialene pracuje, musí byť pravidelne aktualizovaný a zabezpečený heslom.

- Počítač musí mať nainštalovaný antivírusový softvér, ktorý je pravidelne aktualizovaný.
- Prístup iným osobám v domácnosti k počítaču musí byť zamedzený, pre predchádzanie neúmyselného narušenia bezpečnosti informácií.
- Zálohovanie a ukladanie dát pri práci na diaľku prebieha len na vopred schválené úložné médium, ktoré je zašifrované a fyzicky chránené.
- Pri práci na diaľku je potrebné dodržiavať rovnaké pokyny v oblasti bezpečnosti informácií, ako aj pri práci v ambulancii, pokiaľ to povoľujú okolnosti.
- Pokiaľ je to možné, zvážiť použitie virtuálnej privátnej siete a pripájanie cez presne určený port routera.

4.1.2. A.8 Riadenie aktív

A.8.3.1 Správa výmenných médií

Opatrenie:

Vytvoriť a implementovať postupy pre správu médií. Médium musí byť chránené buď fyzicky, alebo musí byť zašifrované. Nezašifrované médiá so zdravotnými informáciami musia byť monitorované. Postupy pre správu médií budú definované v smernici o manipulácii s médiami.

Odporučenie:

- V ambulanciách sa používajú prenosné zálohové médiá obsahujúce osobné, zdravotné údaje pacientov. Takéto médiá musia byť riadne označené a zaevidované.
- Musí byť zaručená fyzická bezpečnosť médií.
- Ak sú obsahom médií osobné, zdravotné informácie, musia byť zašifrované.
- Nepotrebný obsah médií je potrebné odstrániť softvérovými nástrojmi.

A.8.3.2 Likvidácia médií

Opatrenie:

Nepotrebné médiá musia byť zlikvidované, preto je potrebné vytvoriť a implementovať postupy pre ich bezpečnú likvidáciu. Všetky informácie musia byť pred likvidáciou médií

aj iných zariadení bezpečne zmazané alebo zničené. Tieto postupy budú vytýčené v smernici o manipulácii s médiami.

Odporučenie:

- Osoba, ktorá je zodpovedná za likvidáciu obsahu médií, ako aj média samotného, je ich vlastník. Táto zodpovednosť môže byť delegovaná na inú osobu.
- Údaje z média budú vymazané formátovaním, alebo bude použitý softvér na likvidáciu dát.
- Médiá budú likvidované fyzicky, mechanickým znehodnotením, alebo použitím špecializovaného zariadenia na likvidáciu takýchto zariadení u overeného externého dodávateľa.
- Po likvidácii média je potrebné preveriť, či bolo zlikvidované tak, aby sa zamedzilo získaniu akýchkoľvek dát.
- O likvidácii médií, ktoré obsahujú citlivé údaje, je potrebné viesť záznamy.
- Pri poškodených médiách je potrebné zvážiť riziko narušenia dôvernosti informácií o pacientovi pri oprave média.

A.8.3.3 Preprava fyzických médií

Opatrenie:

Je potrebné vytvoriť postupy pre ochranu prenášaných médií proti neoprávnenému prístupu, zneužitiu alebo narušeniu. Tieto postupy budú stanovené v smernici o manipulácii s médiami.

Odporučenie:

- Prepravujú sa len zálohové médiá. Pri ich preprave je potrebné dbať na ich zvýšenú bezpečnosť pri prenose a neustále monitorovať ich stav.
- Dáta na médiách, ktoré sa prenášajú, musia byť zašifrované.

4.1.3. A.9 Riadenie prístupu

A.9.4.3 Systém správy hesiel

Opatrenie:

V organizácii bude zavedený systém správy hesiel, ktorý bude interaktívny a ktorý zaistí použitie kvalitných hesiel. Systém správy hesiel bude zdokumentovaný v smernici o bezpečných heslách. Povinnosti zamestnancov plynúce z tohto opatrenia budú stanovené v smernici o povinnostiach používateľov.

Odporučenie:

- Každý nový používateľ dostane pridelené heslo do operačného systému a ambulantného informačného systému. Za vytvorenie a pridelenie hesiel je zodpovedný lekár, prípadne osoba s delegovanou povinnosťou externej správy IT.
- Je potrebné zabezpečiť, aby minimálny počet znakov prístupového hesla bol osem, aby obsahovalo čísla, špeciálne znaky, veľké a malé písmená. Heslo nesmie mať slovníkový význam a nemôže mať spojitosť s používateľom.
- Heslá nesmú byť rovnaké pre rôzne účty a rôznych používateľov.
- Nové heslo je zakázané zdieľať s personálom či inými osobami, prípadne dodávateľmi, zapisovať ho a nechávať ho viditeľnom mieste.
- Pri krátkodobom odchode od počítača je potrebné, aby ho používateľ uzamkol, pri dlhodobom je potrebné, aby sa odhlásil.
- Heslá budú menené najmenej v intervale pol roka.
- Heslo je potrebné zmeniť pri nebezpečenstve prezradenia hesla.
- Heslá do iných účtov budú menené najmenej v intervale jedenkrát ročne.

4.1.4. A.11 Fyzická bezpečnosť a bezpečnosť prostredia

A.11.2.1 Umiestnenie zariadenia a jeho ochrana

Opatrenie:

Zariadenia budú umiestnené tak, aby boli znížené riziká hrozieb. Pracovné stanice, budú umiestnené tak, aby sa zamedzilo prehliadaniu alebo prístupu subjektov zdravotnej

starostlivosti a verejnosti. Pravidlá pre ochranu zariadení budú stanovené v smernici o fyzickej bezpečnosti zariadení.

Odporučenie:

- Zariadenia sú umiestnené v zabezpečených priestoroch, kam majú prístup len oprávnené osoby a subjekt zdravotnej starostlivosti len za prítomnosti oprávnenej osoby.
- Server, ako aj aktívne sieťové prvky sú, pokiaľ je to možné, uzamknuté v samostatnej miestnosti. Aktívne sieťové prvky sú uzamknuté v dátovom rozvádzači.
- Pokiaľ je to možné, jednotlivé zariadenia sú umiestnené minimálne vo výške 30 cm od zeme, aby sa zamedzilo poškodeniu potopou.

A.11.2.2 Podporné služby

Opatrenie:

Je nutné zaistiť ochranu zariadenia pred zlyhaním napájania a podporných služieb.

Odporučenie:

- Zaistiť, že zariadenia budú vybavené nepretržitým zdrojom napájania UPS a prepäťovou ochranou, čím sa znižuje riziko spojené s poškodením programov, ako aj hardvérových častí zariadení vplyvom kolísania a výpadku elektrickej siete.
- Zvážiť použitie elektrocentrály.
- Zaistiť pravidelné kontroly zariadení UPS, ako aj elektrocentrály. Povinnosť vykonávať tieto kontroly bude zavedená v smernici o fyzickej bezpečnosti zariadení. Zodpovednosť za vykonanie kontroly bude delegovaná na externého správcu IT.

A.11.2.4 Údržba zariadenia

Opatrenie:

Budú zaistené periodické kontroly a pravidelný servis zariadení, aby bolo dosiahnuté správne udržiavanie pre zaistenie dostupnosti a integrity. Pravidlá kontrol budú stanovené v smernici o fyzickej bezpečnosti zariadení. Zodpovednosť za vykonanie kontroly bude

delegovaná na externého správcu IT. Bude vytvorený dokument so zoznamom zariadení, priradenou periodicitou kontrol, záznamom o vykonaní kontroly, a zistených nedostatkoch.

Odporučenie:

- Zavedenie kontroly funkčnosti technických zariadení v pravidelnom intervale najmenej jedenkrát mesačne.
- Zavedenie pravidelných servisných kontrol zariadení podľa odporúčaní dodávateľa.
- Zavedenie pravidelných technických kontrol hardvérových častí zariadení (predovšetkým kontrolu pevného disku počítača s verifikáciou povrchu) špecializovaným servisným technikom v intervale jedenkrát za dva roky.
- Je potrebné viesť záznamy o vykonaných kontrolách.
- Na servis technického zariadenia sú využívané služby externých dodávateľov.
- V prípade potreby vykonania servisu či opravy zariadení mimo priestory ambulancie je potrebné vyžadovať povolenie vlastníka zariadenia a zabezpečiť bezpečnosť osobných zdravotných informácií, pokiaľ ich tieto zariadenia obsahujú.

A.11.2.6 Bezpečnosť zariadení a aktív mimo priestorov organizácie

Opatrenie:

Pre zabezpečenie aktív mimo priestorov ambulancie je potrebné vytvoriť pravidlá, ktoré budú vytýčené v smernici o fyzickej bezpečnosti zariadení. Pri tvorbe pravidiel je potrebné prihliadať na odlišné riziká mimo priestorov ambulancie. Za aktíva mimo priestorov ambulancie zodpovedá ich vlastník, lekár.

Odporučenie:

- Povolenie prenášať aktíva a zariadenia má len vlastník aktív.
- Prenášanými aktívami a zariadeniami zdravotníckeho zariadenia sú predovšetkým notebooky, preto je potrebné dbať na ich zvýšenú ochranu pri prenose mimo priestory ambulancie.
- Je potrebné zabezpečiť, aby boli notebooky chránené dostatočne silným heslom.

- V zariadeniach nesmú byť uložené prístupové heslá k zdravotníckemu informačnému systému, ani k ďalším pracovným účtom.
- Dáta, ktoré sú uložené v notebookoch musia byť šifrované.
- Osoby, ktoré pracujú so zariadeniami mimo priestorov ambulancie, sa riadia pokynmi uvedenými v časti A.6.2.2.

A.11.2.7 Bezpečná likvidácia alebo opakované použitie zariadení

Opatrenie:

Je potrebné stanoviť pravidlá pre bezpečnú likvidáciu zariadení, alebo pre ich opakované použitie. Tieto pravidlá budú stanovené v smernici o fyzickej bezpečnosti zariadení. Zodpovednosť za bezpečnú likvidáciu zariadení má vlastník zariadenia, lekár. Zodpovednosť môže byť delegovaná na externého správcu IT alebo iného externého špecializovaného odborníka. Pred samotnou likvidáciou je potrebné odstrániť všetky zdravotnícke informácie, ako aj softvér.

Odporučenie:

- Údaje zo zariadení budú vymazané formátovaním, alebo bude použitý softvér na likvidáciu dát.
- Zariadenia budú likvidované fyzicky, mechanickým znehodnotením, alebo použitím špecializovaného zariadenia na likvidáciu takýchto zariadení u externého dodávateľa.
- Po likvidácii zariadenia je potrebné preveriť, či bolo zlikvidované tak, aby sa zamedzilo získaniu akýchkoľvek dát.
- O likvidácii zariadení je potrebné viesť záznamy.

A.11.2.9 Zásada prázdneho stola a prázdnej obrazovky monitora

Opatrenie:

Pre zamedzenie narušenia bezpečnosti informácií je potrebné stanoviť a implementovať zásadu prázdneho stola vzhľadom na dokumenty, výmenné médiá a obrazovku monitora. Zásada prázdneho stola bude zdokumentovaná v smernici o povinnostiach používateľov a zamestnanci budú s obsahom smernice preukázateľne zoznámení pri prijatí do zamestnania a každoročne počas pravidelného školenia.

Odporučenie:

- Personál je povinný zabezpečiť, aby aj pri krátkodobom opustení pracoviska, uviedol počítače do stavu, kedy bude pre ďalšie pokračovanie vyžadované prístupové heslo.
- Ak personál opúšťa pracovisko, je povinný korektne sa odhlásiť z počítača.
- Personál je povinný zaistiť, aby neoprávnené osoby nemali vizuálny kontakt s monitorom počítača.
- Personál je povinný zabezpečiť, aby počas poskytovania zdravotnej starostlivosti subjektu neboli v ambulancii voľne prístupné dokumenty obsahujúce osobné údaje iného subjektu.
- Personál je povinný uložiť pred odchodom z pracoviska všetky zdravotné dokumenty do uzamykateľnej kartotéky.

4.1.5. A.12 Bezpečnosť prevádzky

A.12.2.1 Opatrenia proti malvéru

Opatrenie:

Budú vytvorené a zavedené opatrenia pre prevenciu, detekciu a ochranu proti škodlivému softvéru, ktoré budú stanovené v smernici o opatreniach proti malvéru. Rovnako je potrebné aspoň raz ročne vykonať zaškolenie zamestnancov ku zvyšovaniu povedomia na ochranu pred škodlivým softvérom a o stanovených pravidlách. Opatrenia proti malvéru, ktoré musia dodržiavať zamestnanci, budú uvedené v smernici o povinnostiach používateľov.

Odporučenie:

- Počítačová sieť musí byť chránená bránou Firewall.
- Server a pracovné stanice sú chránené antivírusovým softvérom od renomovanej spoločnosti, ktorý je pravidelne aktualizovaný, pre zaistenie efektívnej ochrany pred vírusmi. Rovnako bude zabezpečené správne nastavenie antivírusového programu a výnimky pre mzdové, účtovné a ambulantné softvéry, ktoré budú vyhodnotené ako dôveryhodné.

- Personál ambulancie má zakázané použitie pamäťových médií s neznámym pôvodom, prezeranie a inštaláciu akýchkoľvek nepovolených softvérov.
- Personál musí byť poučený pri používaní internetu ako aj elektronickej pošty tak, aby sa zvyšovalo povedomie na ochranu pred škodlivým softvérom. Musí teda dbať na opatrnosť a predchádzať návštevám podozrivých webových stránok, čítaním podozrivých e-mailov, sťahovaním e-mailových príloh a iných súborov.
- V prípade použitia pamäťových médií, ktoré sa vrátia od iných poskytovateľov zdravotnej starostlivosti, aplikuje pred použitím v systéme minimálne rýchle formátovanie (pri neznámych nosičoch platí zásada, že ich obsah sa neprezerá, nespúšťajú sa z nich žiadne aplikácie, prevedie sa ich formátovanie, ktoré odstráni prípadný malvér). Pri pamäťových médiách, ktoré obsahujú citlivé osobné informácie, scany, videozáznamy a iné zdravotné údaje pacienta za účelom posúdenia zdravotného stavu, vykoná personál prostredníctvom antivírusu najprv scan média, prípadne spustí pamäťové médium na samostatne vyčlenenom počítači, ktorý nie je pripojený v sieti.
- Pri nekorektnom správaní systému technik zabezpečí kontrolu logových súborov, systémovú kontrolu a kontrolu siete.
- Po nekorektnom ukončení alebo výpadku energie vykoná používateľ alebo technik systémovú kontrolu.
- Pri výzve na aktualizáciu systému zabezpečí používateľ alebo technik spustenie stiahnutých aktualizácií v čo najkratšom termíne s dôrazom na bezpečnostné aktualizácie.
- Pri identifikácii malvéru personál urýchlene odpojí počítač od siete a spustí kontrolu ostatných počítačov v sieti na prítomnosť malvéru a ďalej postupuje v súlade s postupmi riešenia incidentov podľa bodu A.16.1.1.

A.12.3.1 Zálohovanie informácií

Opatrenie:

Pre zachovanie stálej dostupnosti dát je potrebné v pravidelných intervaloch vytvárať záložné kópie informácií na pamäťové médiá a ukladať ich vo fyzicky bezpečnom prostredí. Pre zachovanie dôvernosti musia byť údaje na médiách zašifrované. Pravidlá zálohovania dát budú stanovené v smernici o zálohovaní. Za pravidelné vytváranie záloh

bude zodpovedať lekár, alebo osoba s delegovanou právomocou. Rovnako je potrebné zdokumentovať postupy v prípade obnovy zo zálohy.

Odporučenie:

- Vytvoriť evidenciu zálohových médií.
- Zabezpečiť pravidelné zálohovanie databáz a údajov formou inkrementálnej zálohy v rozsahu raz denne na dva nezávislé nosiče (napríklad pevný disk počítača a prenosné pamäťové médium). Pri zálohovaní na viaceré externé pamäťové médiá je vhodné uplatniť cirkuláciu médií a striedať ich.
- Zabezpečiť pravidelné zálohovanie databáz a údajov formou diferenčnej zálohy v rozsahu raz týždenne.
- Zabezpečiť pravidelné zálohovanie databáz a údajov formou úplnej zálohy v rozsahu raz mesačne.
- Minimálne raz mesačne je potrebné overiť stav záloh a možnosť obnovy zo zálohy, za čo zodpovedá externý správca IT.
- Pamäťové médiá je nutné uchovávať vo fyzicky bezpečnom prostredí s dodržaním zásady nenechať zálohové médium neuzamknuté v ambulancii (v prípade odcudzenia počítača aj média dôjde k nenávratnej strate dát).
- Pri prenose zálohových médií na iné miesto je nutné dbať na fyzicky bezpečné prostredie. V domácom prostredí nesmie byť zálohové médium voľne prístupné.

A.12.6.2 Obmedzenie inštalácie softvéru

Opatrenie:

Je potrebné vytvoriť pravidlá pre inštaláciu softvéru zamestnancami, nakoľko existuje možnosť, že daný softvér môže pôsobiť nepriaznivo na bezpečnosť informácií. Pravidlá obmedzenia inštalácie softvéru pre používateľov budú stanovené v smernici o povinnostiach používateľov.

Odporučenie:

- V ambulancii je zakázané inštalovať akýkoľvek softvér bez povolenia vedenia a bez súhlasu správcu IT.
- Inštalovaný softvér musí pochádzať z overeného zdroja.

4.1.6. A.13 Bezpečnosť komunikácií

A.13.1.1 Opatrenia v sieťach

Opatrenie:

Je potrebné vytvoriť pravidlá pre riadenie a kontrolu sietí. Tieto pravidlá budú stanovené v smernici o bezpečnosti komunikácií. Riadenie siete a pravidelné kontroly siete a sieťových prvkov bude vykonávať externý správca IT.

Odporučenie:

- Zodpovednosť za správu a riadenie siete bude mať externý správca IS. Táto povinnosť bude stanovená v jeho pracovnej zmluve.
- Počítačová sieť bude pomocou používateľských mien, hesiel a prístupových práv nakonfigurovaná tak, aby prístup k zdravotným informáciám mali iba oprávnené osoby.
- Bude zamedzené prepojenie informačného systému s verejnou počítačovou sieťou.
- Siete budú zabezpečené prostredníctvom Firewallu. Verejná sieť bude mať nastavené pravidlá na zamedzenie pripojenia k webovým stránkam, ktoré budú vyhodnotené ako potencionálne nebezpečné.
- Správca IT bude robiť pravidelné kontroly siete a sieťových prvkov v intervale najmenej raz za mesiac.

4.1.7. A.16 Riadenie incidentov bezpečnosti informácií

A.16.1.1 Zodpovednosti a postupy

Opatrenie:

Bude navrhnutý systém pre zvládanie incidentov bezpečnosti informácií, postupy a zodpovednosti, ktoré budú stanovené v smernici o riadení informačných incidentov. Bude tiež vytvorený presný postup zvládania incidentov s konkrétnymi krokmi a postupy pre monitorovanie a detekciu a hlásenie správ o udalostiach. Rovnako budú vytvorené postupy pre posudzovanie a rozhodovanie o bezpečnostných udalostiach a zraniteľnostiach. Všetci zamestnanci budú preukázateľne zoznámení s obsahom

smernice pri nástupe do zamestnania, aj pri pravidelných každoročných školeniach. Školenie zamestnancov v tejto oblasti zabezpečí externý špecialista.

Odporučenie:

- Zamestnanci sú pri zistení zraniteľnosti, udalosti, alebo incidentu bezpečnosti informácií povinní tieto bezprostredne nahlásiť vedeniu a externému správcovi IT. Táto povinnosť vychádza z pracovnej zmluvy zamestnanca.
- Správca IT po vyhodnotení situácie rozhodne o potrebných opatreniach a inštruuje zamestnancov, ako postupovať do jeho príchodu.
- Všetky bezpečnostné incidenty je nutné evidovať.

A.16.1.2 Hlásenie udalostí bezpečnosti informácií

Opatrenie:

Podľa postupov pre urýchlené nahlasovanie udalostí bezpečnosti informácií bude určené, ako budú zabezpečené efektívne a včasné odozvy na incidenty. Je potrebné zabezpečiť, aby bol o incidente informovaný aj subjekt zdravotnej starostlivosti, ak sa týka narušenia bezpečnosti jeho osobných údajov. Musí byť vytvorený školiaci plán pre zamestnancov, na základe ktorého budú schopní adekvátne reagovať pri hlásení udalostí. Povinnosť nahlasovať udalosti bude stanovená v pracovných zmluvách zamestnancov. Udalosti budú nahlasované externému správcovi IT.

Odporučenie:

- Hlásenie udalostí je nutné vykonať predovšetkým, ak je zistená neefektívnosť niektorého opatrenia, ak sa zistí nekorektné správanie systému, alebo nesprávna funkčnosť, ak je narušená dôvernosť, integrita, alebo dostupnosť informácií na úrovni, ktorá nie je akceptovateľná, alebo ak je zistené nedodržiavanie stanovených postupov, politík, či smerníc. Rovnako je potrebné nahlasovať udalosti v prípade, že dôjde k ľudským chybám na úrovni, ktorá nebude akceptovateľná pre dodržanie bezpečnosti informácií a pri prelomení opatrení. Ďalej sa riadia pokynmi stanovenými v bode A.16.1.1.
- Ak je narušená bezpečnosť osobných údajov pacienta, je potrebné o tejto skutočnosti pacienta bezprostredne informovať.

A.16.1.3 Hlásenie slabých miest bezpečnosti informácií

Opatrenie:

Zamestnanci používajúci informačné systémy musia monitorovať a hlásiť slabé miesta bezpečnosti informácií. Táto povinnosť je stanovená v pracovných zmluvách zamestnancov.

Odporučenie:

- Zamestnanci monitorujú informačné systémy a sú povinní hlásiť zaznamenané slabé miesta informačných systémov, či nekorektné správanie systému, alebo nesprávnu funkčnosť. Ďalej sa riadia pokynmi stanovenými v bode A.16.1.1.

A.16.1.4 Posúdenie a rozhodnutie o udalostiach bezpečnosti informácií

Opatrenie:

Bude vytvorený systém posudzovania udalostí bezpečnosti informácií pre klasifikáciu incidentov bezpečnosti informácií.

Odporučenie:

- Správca IT posúdi udalosť bezpečnosti informácií pomocou stanovenej klasifikácie a rozhodne, či sa jedná o incident.
- Bezpečnostný incident nastáva, ak boli ohrozené citlivé osobné údaje subjektov zdravotnej starostlivosti, osobné údaje zamestnancov, údaje a aktíva súvisiace s činnosťou vykonávania praxe a podnikania a údaje a aktíva, ktorých strata, zničenie alebo nedostupnosť má za následok finančné škody, alebo zamedzenie poskytovania zdravotnej starostlivosti.

4.1.8. Prehľad opatrení podieľajúcich sa na modifikácií hrozieb

Tabuľka č. 11: Prehľad opatrení podieľajúcich sa na modifikácií hrozieb

(Zdroj: Vlastné spracovanie)

Hrozba	Bezpečnostné opatrenia
Náhodné hrozby	
Prírodné hrozby	
Povodeň	Zníženie zraniteľnosti aktív opatrením A.11.2.1. Dopady na organizáciu sú znížené už zavedenými opatreniami (poistenie).
Požiar	Zníženie pravdepodobnosti výskytu hrozby už zavedenými opatreniami (protipožiarne opatrenia, prístroje). Dopady na organizáciu sú znížené už zavedenými opatreniami (poistenie).
Víchrica	Dopady na organizáciu sú znížené už zavedenými opatreniami (poistenie).
Iná živelná pohroma	Dopady na organizáciu sú znížené už zavedenými opatreniami (poistenie).
Výpadok služieb	
Výpadok elektrickej energie	Zníženie zraniteľnosti aktív opatrením A.11.2.2.
Výpadok internetového pripojenia	Z krátkodobého hľadiska nemá veľký dopad na organizáciu. Riziko je akceptovateľné.
Výpadok IS	Pravdepodobnosť výskytu hrozby znižujú opatrenia A.11.2.2, A.11.2.4 a A.13.1.1. Dopad hrozby znižuje systém zálohovania A.12.3.1. a opatrenie A.16.1.1.
Výpadok bezpečnostného systému	Z krátkodobého hľadiska nemá veľký dopad na organizáciu. Riziko je akceptovateľné.
Technické zlyhania	
Zlyhanie serveru	Pravdepodobnosť výskytu hrozby znižuje opatrenie A.11.2.4.

Zlyhanie pracovnej stanice	Pravdepodobnosť výskytu hrozby znižuje opatrenie A.11.2.4.
Zlyhanie častí ICT infraštruktúry	Pravdepodobnosť výskytu hrozby znižujú opatrenia A.11.2.4 a A.13.1.1.
Zlyhanie medicínskych prístrojov	Pravdepodobnosť výskytu hrozby znižuje opatrenie A.11.2.4.
Poškodenie dát	Dopad hrozby znižuje systém zálohovania A.12.3.1. a opatrenie A.16.1.1. Pravdepodobnosť výskytu hrozby znižujú opatrenia A.11.2.2 a A.11.2.4.
Úmyselné hrozby	
Fyzické hrozby	
Krádež technického vybavenia	Pravdepodobnosť výskytu hrozby znižujú už zavedené opatrenia. Pravdepodobnosť výskytu hrozby čiastočne znižujú opatrenia A.11.2.1 a A.11.2.6.
Krádež médií	Pravdepodobnosť výskytu hrozby znižujú už zavedené opatrenia a opatrenia A.8.3.1. a A.8.3.3. Dopad hrozby znižuje systém zálohovania A.12.3.1.
Krádež dokumentov	Pravdepodobnosť výskytu hrozby znižujú už zavedené opatrenia a čiastočne opatrenie A.11.2.9.
Iné úmyselné hrozby	
Neoprávnený prístup do priestorov	Pravdepodobnosť výskytu hrozby znižujú už zavedené opatrenia.
Neoprávnené získanie prístupových údajov	Pravdepodobnosť výskytu hrozby znižujú opatrenia, A.6.2.2, A.11.2.6, A.11.2.9, A.13.1.1.. Zraniteľnosť aktív znižuje opatrenie A.9.4.3.
Neoprávnené získanie dát	Pravdepodobnosť výskytu hrozby znižujú opatrenia A.6.2.2, A.8.3.3, A.11.2.6, A.11.2.7, A.11.2.9, A.13.1.1., A.12.2.1., A.11.2.1. Zraniteľnosť aktív znižuje opatrenie A.9.4.3.
Zneužitie užívateľského oprávnenia	Pravdepodobnosť výskytu hrozby znižujú už zavedené opatrenia.

Napadnutie ICT	Zraniteľnosť aktív znižujú opatrenia A.13.1.1 a A.9.4.3. Pravdepodobnosť výskytu hrozby znižuje opatrenie A.12.2.1.
Napadnutie IS	Zraniteľnosť aktív znižuje opatrenie A.9.4.3. Pravdepodobnosť výskytu hrozby znižujú opatrenia A.12.2.1. a A.13.1.1.
Získanie dát z vyradených médií	Pravdepodobnosť výskytu hrozby znižujú opatrenia A.8.3.2 a A.11.2.7.
Inštalácia škodlivého softvéru	Zraniteľnosti aktív znižujú opatrenia A.12.2.1 a A.12.6.2. Pravdepodobnosť výskytu hrozby znižujú opatrenia A.6.2.1, A.6.2.2. a A.13.1.1. Dopad hrozby znižuje systém zálohovania A.12.3.1. a opatrenie A.16.1.1.
Zámerné odstraňovanie dát	Dopad hrozby znižuje systém zálohovania A.12.3.1.
Porušenie mlčanlivosti	Pravdepodobnosť výskytu hrozby znižujú už zavedené opatrenia.
Neúmyselné hrozby	
Fyzické hrozby	
Nehoda na pracovisku s následnými škodami	Zraniteľnosť aktív znižuje opatrenie A.11.2.1. Pravdepodobnosť výskytu hrozby znižujú už zavedené opatrenia a opatrenie A.6.1.1.
Strata médií	Pravdepodobnosť výskytu hrozby znižuje opatrenie A.8.3.1 a A.8.3.3. Dopad hrozby znižuje systém zálohovania A.12.3.1.
Iné neúmyselné hrozby	
Chyby personálu pri práci s IS	Dopad hrozby znižuje systém zálohovania A.12.3.1.
Chyby pri nastavení prístupových práv	Pravdepodobnosť výskytu hrozby znižujú opatrenia A.6.1.1 a A.13.1.1.
Chyby pri správe IT služieb	Pravdepodobnosť výskytu hrozby znižuje opatrenie A.6.1.1 a A.13.1.1.

Nedbanlivosť pri údržbe zariadení	Pravdepodobnosť výskytu hrozby znižuje opatrenie A.11.2.4 a čiastočne A.13.1.1.
Nedodržiavanie predpisov pri práci s informáciami	Pravdepodobnosť výskytu hrozby znižujú už zavedené opatrenia a opatrenie A.6.1.1.

4.2. Plán vzdelávania s cieľom zvyšovania povedomia personálu o bezpečnosti informácií

Jednou z najslabších súčastí celého systému informačnej bezpečnosti sú nepochybne zamestnanci, preto je potrebné vytvoriť systém ich vzdelávania v oblasti povedomia o informačnej bezpečnosti a o riešení bezpečnostných udalostí a incidentov, ktorý bude pozostávať zo školení. Plán vzdelávania bude vytvorený ako smernica a povinnosť zúčastňovať sa školení a dodržiavať pravidlá smernice budú zavedené v pracovných zmluvách.

Keďže zamestnanci nemajú odborné vzdelanie v oblasti informačnej bezpečnosti, bude sa vzdelávanie zameriavať predovšetkým na oblasť budovania povedomia o informačnej bezpečnosti, na základné pojmy akými sú dostupnosť, dôvernosť a integrita, zraniteľnosti, hrozby, riziko, udalosti a incidenty, aby mali užívatelia informačných systémov povedomie o tom, ako sa správať, aby nespôsobili vlastnou činnosťou škody. Predovšetkým budú školenia zameriavané tak, aby sa predchádzalo chybám personálu pri práci s informačným systémom. Ďalej následkom, ktoré môže spôsobiť neznalosť práce s internetom a s e-mailom, ako aj dopadom, ktoré vznikajú neodborným narábaním s technickými zariadeniami. Používatelia sa taktiež budú pravidelne oboznamovať s predmetom smerníc a postupov tak, aby okrem teoretických znalostí nadobudli aj praktické, predovšetkým tie, ktoré súvisia s prácou v ambulantnom informačnom systéme a prácou s databázami, ako aj s antivírusovým systémom a v neposlednom rade s operačným systémom. Rovnako je potrebné viesť školenia, ktoré budú smerované na oblasť riadenia incidentov podľa interných smerníc. Odporučené je aj školenie u externých organizácií.

Odporučenie konkrétneho vzdelávacieho systému:

- Zamestnanci budú pri prijatí do zamestnania musieť absolvovať zaškolenie, kde budú zoznámení predovšetkým s bezpečnou prácou v ambulantnom informačnom softvéri.
- Zaškolenie v oblasti práce v ambulantnom informačnom systéme bude vykonávať externý dodávateľ softvéru buď dištančnou formou, alebo osobne.
- Zamestnanci budú pri prijatí do zamestnania musieť absolvovať školenie v oblasti informačnej bezpečnosti, predovšetkým zaškolenie interných bezpečnostných smerníc, pravidiel a plánov, ako aj zaškolenie v oblasti riešení udalostí a incidentov.
- Školenia budú po úvodnom zaškolení opakované v pravidelných intervaloch najmenej raz ročne.

4.3. Plán riadenia incidentov a kontinuita činností

Pre zabezpečenie rýchlej obnovy činností pri bezpečnostnom incidente je potrebné vytvoriť plán, v ktorom budú presne stanovené postupy riadenia incidentov a stratégia obnovy. Plán bude vytvorený primárne na základe výsledkov analýzy rizík pre riziká s neprijateľnou úrovňou, pričom každé bude mať priradené preventívne opatrenia, ako aj činnosti, ktoré bude potrebné vykonať v prípade, že nastane incident, tak aby boli čo najrýchlejšie obnovené zasiahnuté kľúčové procesy. Zamestnanci budú zo všetkých plánov v oblasti riadenia rizík pravidelne školení.

Odporučenia pre zavedenie plánu riadenia incidentov:

- Pravidelné zaškoľovanie zamestnancov v oblasti riadenia a hlásenia incidentov, ktorých povinnosť vychádza z pracovnej zmluvy zamestnanca.
- Zamestnanci budú zaškolení o postupoch, pomocou ktorých môžu samostatne konať v prípade incidentov.
- Postupy budú vypracované vo forme možných krízových scenárov.
- Postupy musia byť pravidelne preskúmavané aspoň raz ročne a vždy po tom, ako nastane incident, aby sa zaručila ich aktuálnosť a adekvátnosť riešenia.

- Zamestnanci budú v prípade výskytu incidentu postupovať podľa rozhodovacieho procesu – zvládnem daný problém riešiť – ak áno, vykonám stanovené postupy a činnosti a nahlásim incident, ak nie, urýchlene nahlásim incident bez zasahovania.
- Bude určená forma nahlasovania incidentov. Nahlasovanie incidentov bude prebiehať telefonicky, prípadne e-mailom priamo externému správcovi IT a poskytovateľovi. Každý incident bude nutné zaevidovať, pričom sa budú vyžadovať údaje, dátum, čas, miesto, popis incidentu, priebeh zásahu, nahlasujúca osoba.

4.4. Prínosy odporúčaných opatrení

V predchádzajúcich kapitolách boli vytýčené opatrenia, ktoré by mali prijať malé zdravotnícke ambulantné zariadenia v snahe o zlepšenie bezpečnosti zdravotníckych informácií. Prínosy, ktoré má zavedenie týchto opatrení okrem zlepšenia informačnej bezpečnosti, sú zvyšovanie povedomia o celej problematike, o hrozbách a rizikách, ktoré pôsobia na informačné aktíva, ale aj zvyšovanie povedomia o opatreniach, ktoré môžu týmto hrozbám zabraňovať, alebo ich minimalizovať. Ignorovaním minimálnych bezpečnostných opatrení, ktoré môžu ambulantné zariadenia prijať, sa vystavujú riziku materiálnej, finančnej, ale predovšetkým legálnej a morálnej škody.

Najväčší prínos, ktorý je spojený s dodržiavaním stanovených opatrení, je zvyšovanie bezpečnosti pacienta a poskytnutie kvalitnejšej zdravotnej starostlivosti.

ZÁVER

Táto práca si kládla za cieľ vytvoriť návrh odporúčaných postupov informačnej bezpečnosti so zameraním na malé zdravotnícke zariadenia. Úvodná časť práce sa zameriavala predovšetkým na vytýčenie teoretických východísk. Boli vysvetlené všeobecné pojmy z oblasti informačnej bezpečnosti, legislatívna a normatívna báza a bol načrtnutý aj systém managementu bezpečnosti informácií. Ako súčasť práce bola vytvorená aj analýza súčasného stavu bezpečnosti informácií v ambulantných zariadeniach a analýza rizík, prostredníctvom ktorej boli vytýčené informačné aktíva, hrozby, ktoré by mohli mať potencionálne vplyv na ich zraniteľnosti a s tým spojené riziká. V praktickej časti práce bol vytvorený zoznam odporúčaných opatrení na základe noriem ISO/IEC 270002 a ISO/IEC 27779, ktoré by mali zdravotnícke zariadenia učiniť pre dodržanie zásad informačnej bezpečnosti.

Napriek tomu, že táto práca nemala za cieľ zavádzať systém managementu informačnej bezpečnosti, boli v teoretickej časti práce vytýčené aj základy problematiky ISMS. Dôvod je práve ten, že na to, aby sme mohli dané opatrenia efektívne aplikovať v praxi v špecifickom prostredí, potrebujeme načrtnúť princípy riadenia celého systému zavádzania bezpečnosti. Celý proces je špecifický práve v tom, že ho každá organizácia prispôsobuje svojim konkrétnym a jedinečným podmienkam. V prípade tak malých organizácií, akými sú spomínané zdravotnícke zariadenia, je však problematické nájsť financie a aj ľudí, ktorých by sme mohli pre účel zavádzania systému informačnej bezpečnosti využiť. Aj z tohto dôvodu bol model analýzy rizík v práci koncipovaný tak, aby sa dal použiť ako ukážkový práve pre malé ambulantné zariadenia. Ponúka ukážku najpravdepodobnejších informačných aktív, zraniteľností a hrozieb, ktoré sa v tomto sektore vyskytujú. Ambulantné zariadenia sa tak môžu dozvedieť, aké príklady potencionálne negatívnych dôsledkov môže mať ignorovanie tejto problematiky na organizáciu, čo môže pôsobiť ako faktor pri rozhodovaní o zavádzaní princípov informačnej bezpečnosti do praxe. Okrem toho môžu organizácie identifikovať príležitosti na zlepšenie klinických, prevádzkových a obchodných oblastí. Zavedenie odporúčaných postupov napomáha organizácii zaistiť bezpečnosť zamestnancov a pacientov, chrániť svoje financie a poskytovať kvalitnú starostlivosť.

ZOZNAM POUŽITÝCH ZDROJOV

(1) ČSN ISO 27000. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017. Triediaci znak 36 9790.

(2) KOCH, M., a kol. *Management informačních systémů*. 3. vyd. Brno: Akademické nakladatelství CERM, s.r.o., 2010. ISBN 97880-214-4157-6.

(3) POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-38-5.

(4) DOUCEK, P., NOVÁK, L., a SVATÁ, V. *Řízení bezpečnosti informací*. 2. vyd. Praha: Professional Publishing, 2011. ISBN 978-807-4310-508.

(5) ČSN ISO 27002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Triediaci znak 36 9798.

(6) HERZIG, W. T., T. WALSH and L. A. GALLAGHER. *Implementing Information Security in Healthcare: Building a Security Program*. Chicago: HIMSS, 2013. ISBN 978-1-938904-34-9.

(7) SMEJKAL, V. a K. RAIS. *Řízení rizik ve firmách a jiných organizacích*: 4., aktualizované a rozšířené vydání. Praha: GRADA Publishing, a.s. 2013. ISBN 978-80-247-4644-9.

(8) ČSN ISO 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Triediaci znak 36 9797.

(9) CALDER, A. a S. WATKINS. *Information Security Risk Management for ISO 27001/ISO 27002*. 3. ed. Cambridgeshire: IT Governance Publishing, 2019. ISBN 978-1-78778-137-5.

(10) ČSN ISO 27005. *Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2019. Triediaci znak 36 9790.

(11) ČSN ISO 27799. *Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2019. Triediaci znak 98 2021.

(12) HERZIG, W. T. (ed.). *Information Security in Healthcare: Managing Risk*. Chicago: HIMSS, 2010. ISBN 978-1-938904-01-1.

(13) POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha: Vydavatelství Policejní akademie ČR, 2007. ISBN 978-8-7251-250-8.

ZOZNAM POUŽITÝCH OBRÁZKOV

ZOZNAM POUŽITÝCH TABULIEK

ZOZNAM POUŽITÝCH SKRATIEK

BYOD	Prines si svoje vlastné zariadenie
ČSN	Česká technická norma
HDD	Pevný disk
IEC	Medzinárodný úrad pre elektrotechniku
ICT	Informačno-komunikačné technológie
IS	Informačný systém
ISMS	Systém managementu bezpečnosti informácií
ISO	Medzinárodná organizácia pre normalizáciu
IT	Informačné technológie
NCZI	Národné centrum zdravotníckych informácií
OECD	Organizácia pre hospodársku spoluprácu a rozvoj
PDCA	Demingov cyklus (plánuj, rob, kontroluj, jednaj)
UPS	Neprerušiteľný zdroj napájania
USB	Univerzálna sériová zbernica
VPN	Virtuálna privátna sieť
VÚC	Vyšší územný celok
WPA	Chránený prístup k Wi-Fi

ZOZNAM POUŽITÝCH PRÍLOH

Príloha I: Bezpečnostná smernica o mobilných zariadeniach

Príloha II: Bezpečnostná smernica o práci na diaľku

Príloha III: Bezpečnostná smernica o manipulácií s médiami

Príloha IV: Bezpečnostná smernica o bezpečných heslách

Príloha V: Bezpečnostná smernica o opatreniach proti malvéru

Príloha VI: Bezpečnostná smernica o zálohovaní

Príloha I

Bezpečnostná smernica

o mobilných zariadeniach

Cieľom týchto opatrení je predchádzať narušeniu bezpečnosti osobných zdravotných informácií, predovšetkým dôvernosti, a rovnako predchádzať možnosti zavlečenia škodlivého kódu, ako aj možnosti poškodenia iných technických zariadení.

Preto je potrebné, aby boli dodržané nasledovné pravidlá:

1. Používateľ má zakázané BYOD, teda využívanie zariadení vo vlastníctve zamestnancov, ak nie sú zabezpečené podľa pokynov.
2. Používateľ zabezpečí, že mobilné zariadenia v jeho vlastníctve budú mať nainštalovaný antivírusový softvér a budú pravidelne aktualizované s dôrazom na bezpečnostné aktualizácie.
3. Používateľ nesmie pripájať mobilné zariadenia do vnútornej siete ambulancie.
4. Používateľ nesmie pripájať mobilné zariadenia k pracovným staniciam.
5. Používateľ nesmie ukladať akékoľvek pracovné údaje na mobilné zariadenia.
6. Používateľ nesmie vytvárať zálohy dát na mobilné zariadenia.
7. Je zakázané, aby sa subjekty zdravotnej starostlivosti pripájali mobilnými zariadeniami na bezdrôtovú sieť ambulancie, pokiaľ neexistuje vyhradená bezdrôtová sieť pre verejnosť.

Riziká spojené s nedodržiavaním princípov stanovených v bezpečnostnej smernici o mobilných zariadeniach môžu spôsobiť ohrozenie bezpečnosti osobných zdravotných informácií, predovšetkým ich dôvernosti, ďalej hrozí možnosť zavlečenia škodlivého kódu a narušenia funkcionality iných technických zariadení.

Táto smernica nadobúda účinnosť od <dátum>.

Príloha II

Bezpečnostná smernica

o práci na diaľku

Cieľom týchto opatrení je predchádzať narušeniu bezpečnosti osobných zdravotných informácií, predovšetkým znižovať hrozbu kybernetických útokov a hrozbu neoprávneného získania prístupu k zariadeniam a informáciám.

Preto je potrebné, aby boli dodržané nasledovné pravidlá:

1. Používateľ pri práci na diaľku z domu musí zaistiť zabezpečenie domácej siete tak, aby bola chránená Firewallom a proxy serverom.
2. Používateľ na ochranu pred neautorizovaným prístupom zabezpečí nastavenie dostatočne silného administrátorského hesla na sieťových prvkoch a rovnako zabezpečí nastavenie dostatočne silným heslom pripojenie na zariadenie v súlade so smernicou o bezpečných heslách.
3. Pre zabezpečenie bezdrôtovej siete pri práci na diaľku musí byť použitý minimálne protokol WPA2 alebo WPA3.
4. Musí byť zaistené nastavenie prístupnosti priečinkov zdieľaných cez sieť len pre presne definovaných používateľov.
5. Operačný systém počítača, na ktorom sa vzdialene pracuje, musí byť pravidelne aktualizovaný a zabezpečený heslom.
6. Počítač, na ktorom používateľ pracuje na diaľku, musí mať nainštalovaný antivírusový softvér, ktorý je pravidelne aktualizovaný.
7. Prístup iným osobám v domácnosti k počítaču musí byť zamedzený, pre predchádzanie neúmyselného narušenia bezpečnosti informácií.
8. Zálohovanie a ukladanie dát pri práci na diaľku prebieha len na vopred schválené úložné médium, ktoré je zašifrované a fyzicky chránené.
9. Pri práci na diaľku je potrebné dodržiavať rovnaké pokyny v oblasti bezpečnosti informácií ako pri práci v ambulancii, pokiaľ to umožňujú podmienky.

10. Pokiaľ je to možné, zvážiť použitie virtuálnej privátnej siete a pripájanie cez presne určený port routera.

Táto smernica nadobúda účinnosť od <dátum>.

Príloha III

Bezpečnostná smernica

o manipulácii s médiami

Cieľom týchto opatrení je predovšetkým znižovať hrozbu straty, poškodenia a odcudzenia médií, či neoprávneného získania údajov z nekorektne zlikvidovaných médií a s tým spojené narušenie dostupnosti, dôvernosti a integrity osobných zdravotných informácií.

Pravidlá pre správu médií:

1. Všetky prenosné zálohové médiá budú označené štítkom a zaevidované v evidencii médií.
2. Právomoc manipulovať s prenosnými zálohovými médiami má prevádzkovateľ.
3. V priestoroch ambulancie je potrebné dbať na zvýšenú fyzickú bezpečnosť médií, preto musia byť uložené v uzamykateľných priestoroch alebo miestach na to určených.
4. Prenosné zálohové média musia byť zabezpečené heslom.
5. Obsah prenosných zálohových médií musí byť šifrovaný.
6. Nepotrebný obsah médií je potrebné odstrániť softvérovými nástrojmi.

Postupy pre bezpečnú likvidáciu médií:

7. Osoba, ktorá je zodpovedná za likvidáciu obsahu médií, ako aj médií samotných, je prevádzkovateľ. Táto zodpovednosť môže byť delegovaná na inú osobu.
8. Pred likvidáciou média budú údaje z média vymazané formátovaním, alebo bude použitý softvér na likvidáciu dát.
9. Médiá budú likvidované fyzicky, mechanickým znehodnotením, alebo použitím špecializovaného zariadenia na likvidáciu takýchto zariadení u overeného externého dodávateľa.
10. Po likvidácii média bude vykonaná kontrola, či bolo médium zlikvidované tak, aby sa zamedzilo získaniu akýchkoľvek dát.

11. O likvidácii médií, ktoré obsahujú citlivé údaje, budú vedené záznamy.
12. Pri poškodených médiách je potrebné zvážiť riziko narušenia dôvernosti informácií o pacientovi pri oprave média, preto prevádzkovateľ najprv posúdi potrebu opravy média u externého dodávateľa. Ak je oprava média nevyhnutná, poskytovateľ zdravotnej starostlivosti zmluvne zaviaže a poučí externého dodávateľa o dodržiavaní bezpečnosti pri narábaní s osobnými zdravotnými údajmi.

Postupy pre ochranu prenášaných médií:

13. Právomoc prenášať médiá má iba prevádzkovateľ zdravotnej starostlivosti.
14. Je povolené prepravovať iba prenosné zálohové médiá.
15. Pri preprave prenosných zálohových médií je potrebné dbať na ich zvýšenú bezpečnosť pri prenose a neustále monitorovať ich stav.
16. Prenosné zálohové médiá musia spĺňať pravidlá pre správu médií.

Táto smernica nadobúda účinnosť od <dátum>.

Príloha IV

Bezpečnostná smernica

o bezpečných heslách

Cieľom týchto opatrení je zaviesť systém správy hesiel a použitie bezpečných hesiel pre zníženie hrozby neoprávneného prístupu k informačným systémom a k informáciám.

Pravidlá pre tvorbu a správu bezpečného hesla:

1. Bezpečné heslo bude mať minimálny počet osem znakov, pričom bude obsahovať čísla, špeciálne znaky, veľké a malé písmená, či iné znaky. Heslo nesmie mať slovníkový význam a nemôže mať spojitosť s používateľom.
2. Každý nový používateľ dostane pridelené heslo do operačného systému a ambulantného informačného systému. Za vytvorenie a pridelenie hesiel je zodpovedný poskytovateľ zdravotnej starostlivosti, prípadne osoba s delegovanou povinnosťou externej správy IT.
3. Heslá nesmú byť rovnaké pre rôzne účty a rôznych používateľov.
4. Pri zmene hesla nesmie byť použité heslo z minulosti.
5. Heslá sa nesmú ukladať v počítačoch, ani zaznamenávať na viditeľných miestach.

Povinnosti používateľov v súvislosti s použitím bezpečných hesiel:

6. Pri podozrení používateľa na nebezpečenstvo prezradenia hesla musí používateľ heslo urýchlene zmeniť.
7. Bezpečné heslo do ambulantného informačného systému musí používateľ zmeniť najmenej v intervale pol roka.
8. Bezpečné heslo do iných účtov musí používateľ zmeniť najmenej v intervale jeden rok.
9. Používateľ sa pri tvorbe nového hesla musí riadiť princípmi tvorby bezpečného hesla.
10. Používateľ nesmie v informačných systémoch a pracovných účtoch používať heslá, ktoré používa v iných súkromných účtoch.

11. Používateľ nesmie zdieľať heslo s personálom, či inými osobami a dodávateľmi služieb.
12. Používateľ nesmie uchovávať heslo na viditeľných miestach (napr. na papieri na stole, monitore).

Táto smernica nadobúda účinnosť od <dátum>.

Príloha V

Bezpečnostná smernica

o opatreniach proti malvéru

Cieľom týchto opatrení je zaistiť prevenciu, detekciu a ochranu proti škodlivému softvéru.

Pravidlá pre ochrana proti malvéru:

1. Server a pracovné stanice sú chránené antivírusovým softvérom od renomovanej spoločnosti, ktorý je automaticky pravidelne aktualizovaný, pre zaistenie efektívnej ochrany pred vírusmi.
2. Počítačová sieť musí byť chránená bránou Firewall.
3. Za inštaláciu, aktualizácie a za správne nastavenie antivírusového programu (tak, aby boli vytvorené výnimky pre mzdové, účtovné a ambulantné softvéry, ktoré budú vyhodnotené ako dôveryhodné), ako aj Firewallu je zodpovedný externý správca IT.
4. Za urýchlené riešenie problémov spojených s podozrením na malvér je zodpovedný externý správca IT.
5. Pri nekorektnom správaní systému externý správca IT zabezpečí kontrolu logových súborov, systémovú kontrolu a kontrolu siete.
6. Po nekorektnom ukončení alebo výpadku energie vykoná používateľ alebo technik systémovú kontrolu.

Postupy pri podozrení z nakazenia malvérom:

7. Pri zistení nákazy vírusom používateľ urýchlene odpojí počítač od siete a spustí kontrolu ostatných počítačov v sieti na prítomnosť malvéru a ďalej postupuje v súlade s postupmi riešenia incidentov a podľa pokynov externého správcu IT.
8. Do príchodu externého správcu IT na pracovisko používatelia nesmú manipulovať s pracovnou stanicou.

Povinnosti používateľov v súvislosti s ochranou proti malvéru:

9. Používatelia majú zakázané akýmkoľvek spôsobom meniť konfiguráciu antivírusového softvéru.
10. Používatelia majú zakázané použitie pamäťových médií s neznámym pôvodom, prezeranie a inštaláciu akýchkoľvek nepovolených softvérov.
11. Používateľ je povinný ohlásiť akékoľvek nekorektné správanie a podozrenie na nesprávne fungovanie antivírusového systému externému správcovi IT.
12. V prípade použitia prenosných pamäťových médií, ktoré sa vrátia od iných poskytovateľov zdravotnej starostlivosti, aplikuje používateľ pred použitím v systéme minimálne rýchle formátovanie (pri neznámych nosičoch platí zásada, že ich obsah sa neprezerá, nespúšťajú sa z nich žiadne aplikácie, prevedie sa ich formátovanie, ktoré odstráni prípadný malvér). Pri pamäťových médiách, ktoré obsahujú citlivé osobné informácie, scany, videozáznamy a iné zdravotné údaje pacienta za účelom posúdenia zdravotného stavu, vykoná používateľ kontrolu média na prítomnosť vírusov prostredníctvom antivírusového programu.
13. Používatelia majú povolené používanie internetu za pracovným účelom, pričom musia dbať na opatrnosť a predchádzať návštevám podozrivých webových stránok a sťahovaním podozrivých súborov a softvérov.
14. Používateľ musí dbať na zvýšenú opatrnosť pri prijímaní elektronickej pošty, predovšetkým príloh, ktoré sú podozrivé a môžu byť potencionálnym zdrojom malvéru, preto je zakázané otvárať takúto poštu, pokiaľ používateľ nepozná odosielateľa, alebo mu nie je aspoň čiastočne známy obsah správy.

Táto smernica nadobúda účinnosť od <dátum>.

Príloha VI

Bezpečnostná smernica

o zálohovaní

Cieľom týchto opatrení je zabezpečiť kvalitný systém zálohovania dát, ktorý bude zaručovať stálu dostupnosť dát v prípade výpadku alebo poškodenia informačných systémov.

Pravidlá pre zálohovanie dát:

1. Všetky dáta ambulantného informačného systému, ako aj iné potrebné údaje musia byť zálohované v takom rozsahu, aby pri strate údajov bola možná úplná obnova informačných systémov.
2. Všetky zálohy, ktoré obsahujú osobné zdravotné údaje, budú šifrované.
3. Za vytvorenie záloh je zodpovedný poskytovateľ zdravotnej starostlivosti.
4. Pravidelné zálohovanie databáz a údajov formou inkrementálnej zálohy bude vykonané v rozsahu raz denne na dva nezávislé nosiče (napríklad pevný disk počítača a prenosné pamäťové médium). Pri zálohovaní na viaceré externé pamäťové médiá bude uplatnená cirkulácia médií a ich striedanie.
5. Pravidelné zálohovanie databáz a údajov formou diferenčnej zálohy bude vykonané v rozsahu raz týždenne.
6. Pravidelné zálohovanie databáz a údajov formou úplnej zálohy bude vykonané v rozsahu raz mesačne.
7. Minimálne raz mesačne bude overovaný stav záloh a možnosť obnovy zo zálohy, za čo zodpovedá externý správca IT. Postupy pri obnove zo zálohy sú zabezpečené poskytovateľom ambulantného informačného systému.
8. Na médiách budú uchovávané zálohy minimálne po dobu dvoch období zálohovania.
9. Pamäťové médiá budú uchovávané vo fyzicky bezpečnom prostredí s dodržaním zásady nenechať zálohové médium neuzamknuté v ambulancii (v prípade odcudzenia počítača aj externého zálohového média dôjde k nenávratnej strate dát).

10. Pri prenose zálohových médií na iné miesto nutné dbať na fyzicky bezpečné prostredie. V domácom prostredí nesmie byť zálohové médium voľne prístupné.
11. Poskytovateľ zdravotnej starostlivosti bude viesť evidenciu zálohových médií.

Táto smernica nadobúda účinnosť od <dátum>.